L1: Entry 1 of 2 File: JPAB Dec 14, 1999

PUB-NO: JP411345266A
DOCUMENT-IDENTIFIER: JP 11345266 A
TITLE: METHOD AND SYSTEM FOR MANAGING APPLICATION FOR MULTI-FUNCTION SMART CARD

PUBN-DATE: December 14, 1999

INVENTOR-INFORMATION:

NAME	COUNTRY
PAN, JACK C	
GUZMAN, MARC A	
BOYD, NIK	
SMUSHKOVICH, YOSIF	
PINN, FRED	

ASSIGNEE-INFORMATION:

NAME	COUNTRY
CITICORP DEV CENTER INC	

APPL-NO: JP11085526
APPL-DATE: March 29, 1999

INT-CL (IPC): G06 F 17/60; G06 F 9/445; G06 F 19/00

ABSTRACT:

PROBLEM TO BE SOLVED: To allow a card owner to easily access financing and other services by installing a monitor application on a master card, authenticating download of a new application and downloading the new application to the master card.

SOLUTION: A card owner 24 selects one applet from an applet list. When a monitor application for the selected applet does not exist on a card 2, a new applet is downloaded from an applet server in an electronic customized depot 26. When the new monitor application is added to the card 2, it is initialized by plural necessary keys obtained from a security server in the depot 26. And, the selected applet is downloaded from the applet server and is installed by using a security mechanism of the monitor application and, e.g. a gatekeeper function.

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（A）　(11)特許出願公開番号

特開平11－345266

(43)公開日　平成11年(1999)12月14日

(51)Int.Cl.[6]	識別記号	FI	
G06F 17/60		G06F 15/21	340Z
9/445		9/06	420J
19/00		15/30	330
			350A

審査請求　未請求　請求項の数1　OL　外国語出願　（全 69 頁）

(21)出願番号　特願平11－85526

(22)出願日　平成11年(1999)３月29日

(31)優先権主張番号　60／079803

(32)優先日　1998年３月30日

(33)優先権主張国　米国（US）

(71)出願人　598156527
シティコープ　デヴェロップメント　センター，インコーポレイテッド
Ｃｉｔｉｃｏｒｐ　Ｄｅｖｅｌｏｐｍｅｎｔ　Ｃｅｎｔｅｒ，Ｉｎｃ．
アメリカ合衆国　カリフォルニア州　90066，ロスアンジェルス，ダヴリュー．ジェファーソン　ブールバード　12731

(72)発明者　ジャック　シー．パン
アメリカ合衆国　カリフォルニア州　91748，ロウランド　ハイツ，サウス　ノリッジ　プレイス　3651

(74)代理人　弁理士　古谷　栄男　（外３名）

最終頁に続く

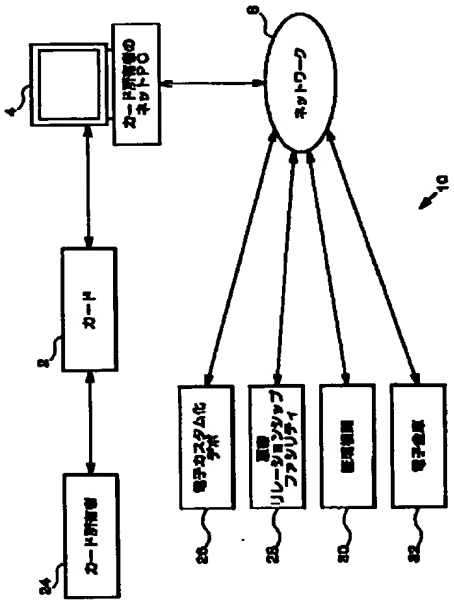
(54)【発明の名称】　多重機能スマートカード用アプリケーションを管理する方法およびシステム

(57)【要約】　（修正有）

【課題】　多重機能スマートカード用のアプリケーションを管理するための方法を提供する。

【解決手段】　スマートカード・マイクロコンピュータのマスター・アプリケーションとインストールされたひとつ以上のモニター・アプリケーションを使用し、スマートカードへ新規アプリケーションのダウンロードを認証し、管理する。新規アプリケーションは、モニター・アプリケーションのセキュリティ・メカニズムを使用して、スマートカード上にインストールされる。新規アプリケーションがインストールされる時、オブジェクト指向の分類に従がってスマートカードのソフトウエア・レジストリに登録され、レジストリのコピーは電子貸金庫に保管され、そして、電子貸金庫は新規アプリケーション用の操作データでもって更新される。

図3



1

【特許請求の範囲】

【請求項1】カード所有者のための多重機能スマートカードへの少なくともひとつの新規アプリケーションの追加を管理する方法であって：スマートカードのマイクロコンピュータ上に新規アプリケーションのためのモニター・アプリケーションをインストールすること；前記スマートカード上に存在するモニター・アプリケーションにより、およびマスター・アプリケーションにより新規アプリケーションのダウンロードを認証すること；および前記スマートカードマイクロコンピュータへ前記新規アプリケーションをダウンロードすること；を含む方法。

【請求項2】前記モニター・アプリケーションをインストールすることが、更にサーバーからモニター・アプリケーションをダウンロードすることを含む、
請求項1の方法。

【請求項3】前記サーバーが、更に電子カスタム化デポを備える、
請求項2の方法。

【請求項4】前記電子カスタム化デポが、更にアプレット・サーバーとモニター・アプリケーション・サーバーの少なくとも一方の機能性を備える、
請求項3の方法。

【請求項5】前記モニター・アプリケーションをインストールすることが、更に端末で前記モニター・アプリケーションをダウンロードすることを含む、
請求項1の方法。

【請求項6】前記端末が更に、現金自動預払機、販売店端末、パソコン、個人用情報機器、TVセット・トップ・ボックス、ランドフォン、セルフォン、デジタルフォン、ケーブルTV受像器、衛星TV受像器、接触式読取装置、非接触式読取装置、および接触・非接触組合せ式読取装置から成るグループから選択されたスマートカード・アクセス装置を備える、
請求項5の方法。

【請求項7】前記新規アプリケーションをダウンロードすることが更に、前記端末に接続されたサーバーから、電子ワレットのための複数の機能性の少なくとも一部分から成るアプリケーションをダウンロードする一方、前記電子ワレットのための機能性の他の部分が、前記端末と前記サーバーの少なくとも一方に、移動する形式で残るようにすることを含む、
請求項6の方法。

【請求項8】前記モニター・アプリケーションをインストールすることが更に、ネットワークを通してモニター・アプリケーションをダウンロードすることを含む、
請求項1の方法。

【請求項9】前記ネットワークが更に、公衆回路および専用回路の少なくとも一方を含む、請求項8の方法

【請求項10】前記ダウンロードを認定することが更に、前記モニター・アプリケーションを初期化することを含む、
請求項1の方法。

2

【請求項11】前記モニター・アプリケーションを初期化することが更に、サーバーにより提供されるキーにより、前記モニター・アプリケーションを初期化することを含む、
請求項10の方法。

【請求項12】前記ダウンロードを認証することが更に、前記モニター・アプリケーションでもって前記新規アプリケーションのためのアプリケーション識別子を登録することを含む、
請求項1の方法。

【請求項13】前記新規アプリケーションをダウンロードすることが更に、前記カード所有者の識別を確認することを含む、
請求項1の方法。

【請求項14】前記識別を確認することが更に、前記スマートカードマイクロコンピュータ上のアプリケーションにより、前記識別を確認することを含む、
請求項13の方法。

【請求項15】前記識別を確認することが更に、前記カード所有者のPINでもって識別確認することを含む、
請求項14の方法。

【請求項16】前記識別を確認することが更に、前記カード所有者のバイオデータでもってアイデンティフィケーション（身分証明）をベリファイ（確認）することを備える請求項14の方法。

【請求項17】前記識別を確認することが更に、端末でスキャナーでもって前記バイオデータを確認することを含む、
請求項16の方法。

【請求項18】前記バイオデータを確認することが更に、前記スマートカードマイクロコンピュータ上の基準テンプレートと前記バイオデータを照合することを含む、
請求項17の方法。

【請求項19】前記バイオデータは、更に前記カード所有者に関する指紋データを含む、
請求項18の方法。

【請求項20】前記新規アプリケーションをダウンロードすることが更に、前記スマートカードを認証することを含む、
請求項1による方法。

【請求項21】前記スマートカードを認証することが更に、サーバーにより前記スマートカードを認証することを含む、
請求項20による方法。

【請求項22】前記新規アプリケーションをダウンロードすることが更に、前記カード所有者にサービス・オプ

ションの選択を提示することを含む、
請求項1による方法。
【請求項23】前記新規アプリケーションをダウンロードすることが更に、前記カード所有者がサービス・オプションを選択して新規アプリケーションをダウンロードすることを含む、
請求項22による方法。
【請求項24】前記新規アプリケーションをダウンロードすることが更に、カード所有者に、有資格の新規アプリケーションのリストを提示することを含む、
請求項1による方法。
【請求項25】前記有資格の新規アプリケーションのリストが更に、予め決められたパラメータに従う複数の新規アプリケーションを含む、
請求項24による方法。
【請求項26】前記予め決められたパラメーターは、カード所有者との関係に基づくビジネスによりサポートされる新規アプリケーション、および前記スマートカードマイクロコンピュータ上で利用可能なスペースにクラスタとして適合する新規アプリケーションの少なくとも一方を含む、
請求項25による方法。
【請求項27】前記予め決められたパラメーターは更に、前記アプリケーションが依存する他の何れかのアプリケーションとともに、前記スマートカードマイクロコンピュータ上で利用可能なスペースに従属クラスターとして適合する前記新規アプリケーションを含む、
請求項26による方法。
【請求項28】前記新規アプリケーションをダウンロードすることが更に、前記カード所有者によりアプリケーションの前記リストから前記新規アプリケーションを選択することを含む、
請求項24による方法。
【請求項29】前記新規アプリケーションをダウンロードすることが更に、サーバーから前記新規アプリケーションをダウンロードすることを含む、
請求項1による方法。
【請求項30】前記サーバーが、更に電子カスタム化デポを備える、
請求項29による方法。
【請求項31】前記電子カスタム化デポが更にアプレット・サーバーおよびモニター・アプリケーション・サーバーの少なくとも一方の機能性を備える、
請求項30による方法。
【請求項32】前記新規アプリケーションをダウンロードすることが、端末で新規アプリケーションをダウンロードすることを含む、
請求項1による方法。
【請求項33】前記端末が更に、現金自動預払、販売店端末、パソコン、個人用情報機器、TVセット・トップ・ボックス、ランドフォン、セルフォン、デジタルフォン、ケーブルTV受像器、衛星TV受像器、接触式読取装置、非接触式読取装置、および接触・非接触組合せ式読取装置から成るグループから選択されたスマートカード・アクセス装置を備える、
請求項32による方法。
【請求項34】前記新規アプリケーションをダウンロードすることが更に、ネットワークを通して新規アプリケーションをダウンロードすることを含む、
請求項1による方法。
【請求項35】前記ネットワークが更に、公衆回路および専用回路の少なくとも一方を備える、
請求項34による方法
【請求項36】前記新規アプリケーションをダウンロードすることが更に、前記スマートカードマイクロコンピュータ上に新規アプリケーションをインストールすることを含む、
請求項1による方法。
【請求項37】前記新規アプリケーションをインストールすることが更に、前記モニター・アプリケーションのセキュリティ・メカニズムを使用して前記新規アプリケーションをインストールすることを備える、
請求項36による方法。
【請求項38】前記新規アプリケーションをインストールすることが更に、操作キーでもって前記新規アプリケーションを供給することを含む、
請求項36による方法。
【請求項39】前記新規アプリケーションをインストールすることが更に、カード所有者情報でもって前記新規アプリケーションを供給することを含む、
請求項36による方法。
【請求項40】前記新規アプリケーションをインストールすることが更に、デジタル証明書でもって前記新規アプリケーションを供給することを含む、
請求項36による方法。
【請求項41】前記新規アプリケーションをインストールすることが更に、前記スマートカードのソフトウエア・レジストリに、前記新規アプリケーションを登録することを含む、
請求項36による方法。
【請求項42】前記新規アプリケーションを登録することが更に、前記ソフトウエア・レジストリのオブジェクト指向分類に従がって前記新規アプリケーションを登録することを含む、
請求項41による方法。
【請求項43】前記新規アプリケーションを登録することが更に電子貸金庫へ前記スマートカード・ソフトウエア・レジストリのコピーを与えることを含む、
請求項41による方法。
【請求項44】前記コピーを備え付けることが更に、前

記新規アプリケーションのためのオペレーションデータのコピーでもって電子貸金庫を更新することを含む、
請求項43による方法。
【請求項45】前記新規アプリケーションをインストールすることが更に、前記スマートカード上で、前記新規アプリケーションの少なくともひとつのオブジェクトと、もうひとつのアプリケーションの少なくともひとつのオブジェクトと、選択的に共有することを含む、
請求項36による方法。
【請求項46】前記選択的に共有することが更に、前記新規アプリケーションによる前記オブジェクトの限定的な共有、および前記新規アプリケーションによる非限定的な共有、の少なくとも一方を含む、
請求項45による方法。
【請求項47】カード所有者のための多重機能スマートカードへ少なくともひとつの新規アプリケーションを確実に追加するためのシステムであって：前記スマートカードのマイクロコンピュータ上に前記新規アプリケーションのためのモニター・アプリケーションをインストールする手段；前記スマートカード上に在住する、モニター・アプリケーションにより、およびマスター・アプリケーションにより、前記新規アプリケーションのダウンロードを認証するための前記インストール手段に関連付けられた手段；　そして、前記スマートカードマイクロコンピュータへ前記新規アプリケーションをダウンロードするための前記認定手段に関連付けられた手段：を備えるシステム。
【請求項48】前記インストール手段が更に、サーバーから前記モニター・アプリケーションをダウンロードする手段を備える、
請求項47によるシステム。
【請求項49】前記サーバーが更に電子カスタム化デポを備える、
請求項48によるシステム。
【請求項50】前記電子的カスタム化デポが更に、アプレット・サーバーおよびモニター・アプリケーション・サーバーの少なくとも一方の機能性を備える、
請求項49によるシステム。
【請求項51】前記モニター・アプリケーションをダウンロードする前記手段が更に、ネットワークを通し前記サーバーと通信する端末を備える、
請求項48によるシステム。
【請求項52】前記新規アプリケーションをダウンロードする前記手段が更にサーバーを備える、
請求項47によるシステム。
【請求項53】前記サーバーが更に電子カスタム化デポを備える、
請求項52によるシステム。
【請求項54】前記電子カスタム化デポが更に、アプレット・サーバーおよびモニター・アプリケーション・サーバーの少なくとも一方の機能性を備える、
請求項53によるシステム。
【請求項55】前記新規アプリケーションをダウンロードする前記手段が更に、ネットワークを通し前記サーバーと通信する端末を備える、
請求項52によるシステム。
【発明の詳細な説明】
【0001】
【関連出願とのクロスリファレンス】本出願は、1998年3月30日出願の米国特許仮出願第60／079，803号の優先権を請求する。
【0002】
【発明の分野】本発明は、一般的にスマートカードに関し、更に詳細には、2つ以上のスマートカード機能のための処理能力と記憶容量とを有するチップベース・スマートカード用のアプリケーションを管理する方法およびシステムに関する。
【0003】
【発明の背景】プラスチックカード上に磁気的ストライプを持つ単機能磁気的ストライプカードが、長年にわたり使用されてきた。そのようなカードは磁気的ストライプ技術に基づいており、カード所有者の名前、口座番号、有効期限等の情報を含む、例えば40キャラクタまでのデータを3トラック上に留めることができる。既存のクレジットカード、デビットカード、およびテレフォンカードは磁気的ストライプをベースとしている。
【0004】例えば、8051または6805のような8ビット・マイクロプロセッサをプラスチックカードに埋め込んだ単機能チップ・カードは、限られた処理能力と、例えば1から2KのE² PROMの限られた記憶容量とを提供する。そのようなカードは、単機能をサポートし、磁気的ストライプカードを凌駕して、偽造され難いハードウエアによる良好なセキュリティ、そしてオンライン・トランザクションおよびインフラストラクチャーのコストを削減する。そのようなカードの内容は、発行の時点で固定される。
【0005】多重技術ハイブリッドカードは、2つ以上のカード技術を単一のカード内に混成する。そのようなカードに適用される技術には、磁気的ストライプ、2次元バーコード、光学的ストライプ、およびチップが含まれている。このような組合せの背景にある理由は、磁気的ストライプの互換性(backword compatibility)や、2次元バーコードまたは光学的ストライプの記憶容量を用いて、チップの処理パワーをてこ入れすることである。チップとの光学的組合せについては、組合せ読取装置が、カードのチップ部と光学的ストライプ部の両方を読出しかつ書込むことができる。
【0006】別のカードでは、接触技術と非接触技術が組合わされている。非接触式カードは機能的には接触式カードを同じであるが、カード読取装置とのやりとり(i

nteract)には、装置へ挿入するのでなく無線周波技術を用いている。非接触技術を伴なうカードは、読取装置から1mm以内（密結合）、8～10cm（近接）、または0．5～1m（近傍）に入った時、トランザクション・データを伝送するとともに、受取ったデータを記録する。非接触式カードを用いたトランザクション時間は、装置へ挿入する必要のあるカードと比較して、1／20から1／30に減少する。そのような組合せカードは、非接触式カードの利便性、性能、信頼性を、接触式カードが持つセキュリティと機能とともに提供する。これらのカードは、バス、列車、地下鉄、フェリー等の機関へのアクセスや大量輸送用途として人気を得、特に単一カードでの支払い方法と組合わされた時、実用的なスマートカード用途として出現した。

【0007】スタティック多重機能チップ・カードは、カードの初期化時にE² PROMにマスキングされた多重機能を扱う能力はあるが、一旦カードが発行されればアプリケーションや機能は固定されるので、これらのカードはスタティックである。

【0008】スマートカード業界ができたのは、ほぼ1970年代以降であった。しかし、ヨーロッパを除いて、世界の大部分では試行やパイロットの域を出ることはなかった。例えば、銀行などの金融機関はVISA CASHやMONDEXのようなストアード・バリュー・カード（汎用プリペイドカード：stored value cards）を、パイロット計画で顧客と販売店に発行した。そのようなパイロット試験計画では、ストアード・バリュー・カードが、顧客と販売店のマーケットでの受入臨界数に達するのを支援するために、そして販売時点情報管理（POS）端末での相互運用を確かなものにするために、人口密度の高い地域でテストされた。

【0009】スマートカード利用率の増加は希望を与えてはいるが、ストアード・バリュー・カードやテレフォンカードのような単機能スマートカードが米国では販売し難いことも明らかである。これは主として、現金の便利さと、クレジットカードの普及とが原因である。従って、ストアード・バリュー用途は、せいぜい、実社会でのスマートカード計画の必要な要素であるアプリケーションと考えられるが、スマートカードの受入臨界量を創り上げるには、それだけでは不十分である。

【0010】スマートカード業界の、1970年代のその発端以降、最初の動きは、チップベースのプラスチック・カードが開発されて、対応する磁気的ストライプと置き換わり、この技術が発生するとともに始まった。そのようなカードは、オンライン・トランザクションおよびその基礎をなすインフラ・サポートに関連するセキュリティを高め、かつコストを削減した。ダイナミック多重機能スマートカードの出現で、スマートカード業界での第2の動きが始まっている。

【0011】米国は第1の動きに活発に関係することはほとんどなかった。それは、遠隔通信インフラが確立されていたこと、そしてクレジットカードの利用が普及していたからである。しかし、米国は第2の動きのリーダーになり得る。というのは、スマートカードに必要とされる携帯性、セキュリティ、暗号化、および認証を提供することに対するエレクトロニック・コマース業界の信頼があるからである。Javaカード・プラットフォームのような技術の開発は、「一度書込めば、どこでも走る」という利点の実現を、スマートカード業界で可能にするが、そこでアプリケーションが必要とするのは、一度だけ書込むことであり、そうすればどのメーカーのどのカードでも動作することができる。

【0012】

【発明の概要】本発明の特徴と利点は、多重機能スマートカード用アプリケーションを管理する方法およびシステムを提供することであり、カード所有者が所持する現金を少なくでき、またカード所有者が任意に、金融や他のサービスへ何時何処でも、どんな装置を経由してもアクセスを可能にすることである。

【0013】本発明の更なる特徴と利点は、多重機能スマートカード用アプリケーションを管理する方法およびシステムを提供することであり、カード所有者が個人情報をオーガナイズすることを可能にする。

【0014】本発明の追加の特徴と利点は、多重機能スマートカード用アプリケーションを管理する方法およびシステムを提供することであり、カード所有者が所持するカードを少なくでき、また同一カードを使って一連のアプリケーションを行なうことを可能にする。

【0015】本発明の別の特徴と利点は、多重機能スマートカード用アプリケーションを管理する方法およびシステムを提供することであり、カード所有者に、カード上の自らの価値（バリュー）ある情報をバックアップする手段を提供する。

【0016】本発明のより更なる特徴と利点は、多重機能スマートカード用アプリケーションを管理する方法およびシステムを提供することであり、カード所有者が、例えば、緊急時情報や保険情報等、あらゆるタイプの情報をカードに記憶させることを可能にする。

【0017】本発明のより更なる特徴と利点は、多重機能スマートカード用アプリケーションを管理する方法およびシステムを提供することであり、カード所有者が、個人のニーズと好みに基づきアプリケーションを選択することにより、前記アプリケーションをカスタム化することが可能になる。

【0018】本発明の上記の、そして他の特徴、利点、目的を達成するために、本発明の実施形態は、カード所有者のためにスマートカードへ新規なアプリケーションまたはアプレットを追加するような、多重機能スマートカード用アプリケーションを管理する方法およびシステムを提供し、例えば、スマートカードのマイクロコンピ

ュータに、新規アプリケーションのためのモニター・アプリケーションをインストールすること、スマートカード上に在るモニター・アプリケーションおよびマスター・アプリケーションにより新規アプリケーションのダウンロードを認証すること、および、スマートカードのマイクロコンピュータへ新規アプリケーションをダウンロードすること、を含む。システムの主要なハードウエア構成要素は、例えば、マイクロコンピュータを埋め込んだスマートカード、端末、ネットワーク、金融機関サーバー等のサーバー、を含む。カードアプリケーション・プラットフォームの重要な側面は、マスター・アプリケーションとモニター・アプリケーションである。マスター・アプリケーションはスマートカード上で、アービター(arbiter)、ゲートキーパ(gatekeeper)、メッセージデスパッチャ(message dispatcher)として使用し、モニター・アプリケーションは、アプレット・プロバイダにより供給される特殊なアプレットであり、これはプロバイダのひとつまたは複数アプレットを、スマートカード上へのインストールすることを制御する。

【００１９】本発明の実施形態において、モニター・アプリケーションは、例えば、電子的カスタム化デポ（electronic customization depot）のようなサーバーから、モニター・アプリケーションをダウンロードすることによりインストールする。そのデポは、アプレット・サーバーまたはモニター・アプリケーション・サーバーの一方または両方の機能を含む。モニター・アプリケーションは、例えば、端末でダウンロードされ、端末は、現金自動預払機（automated teller machine : ATM）、販売店端末、パソコン、個人用情報機器（personal digital assistant : PDA）、ＴＶのセット・トップ・ボックス（TV set-top box）、ランドフォン(land phone)、セルフォン(cell phone)、デジタルフォン(digital phone)、ケーブルＴＶボックス(cable TV box)、衛星ＴＶボックス(satelite TV box)、接触式読取装置、非接触式読取装置、接触・非接触式読取装置など、多数のアクセス装置の何れかひとつである。モニター・アプリケーションは、例えば、公衆または専用の回線を通じ、端末においてサーバーからダウンロードされる。いずれの場合も、スマートカードの初期化中に、あるいはスマートカードが発行された後に、例えばサーバーが提供するキーによって、モニター・アプリケーションを初期化することは、新規アプリケーションのダウンロードを認証することの一つの側面である。新規アプリケーションのダウンロードを認証することの他の側面は、モニター・アプリケーションにより、さらにそれに続いてメッセージデスパッチ用のマスター・アプリケーションにより、アプリケーションＩＤ（識別子）を新規アプリケーションのために登録することである。

【００２０】本発明の実施形態において、スマートカードへ新規アプリケーションをダウンロードする際のセキュリティの観点は、カード所有者のＩＤを、例えば、スマートカードのマイクロコンピュータ上のアプリケーションにより確認することである。そのような識別は、例えばカード所有者のＰＩＮにより、またはカード所有者の生体的データ（biometric data）でなされる。後者は、例えば、端末でスキャナにより実行され、カード所有者の指紋のような生体的データが、スマートカード上の基準テンプレートと比較される。新規アプリケーションをダウンロードする際のセキュリティの他の観点は、スマートカードを、例えばサーバーで認証することである。

【００２１】本発明の実施形態において、カード所有者は、カード所有者のスマートカードに新規アプリケーションをダウンロードするオプションも含め、システムによりサービス・オプション選択が提供される。新規アプリケーションをダウンロードするオプションを選択すると、予め決められたパラメータに従って、選択すべき適格な新規アプリケーションのリストが、カード所有者に提供される。予め決められたパラメータには、例えば、特定の新規アプリケーションはカード所有者と金融機関の間の関係に基づくビジネスによりサポートされているか、そして、スマートカードのマイクロコンピュータ上に特定の新規アプリケーションを収容する十分なスペースがあるか、が含まれる。

【００２２】本発明の実施形態において、カード所有者は、適格な新規アプリケーションのリストから新規なカードアプリケーションを選択し、そしてその新規アプリケーションは、アプレット・サーバーおよびモニター・アプリケーション機能の一方または両方を持つ電子的カスタム化デポ等のサーバーから、スマートカードにダウンロードされる。新規アプリケーションは端末でダウンロードされるが、この端末は、現金自動預払機（ＡＴＭ）、販売店端末、パソコン、個人用情報機器、ＴＶのセット・トップ・ボックス、ランドフォン、セルフォン、デジタルフォン、ケーブルＴＶボックス、衛星ＴＶボックス、接触式読取装置、非接触式読取装置、接触・非接触組合せ式読取装置等の、スマートカードのアクセス装置のいずれかである。

【００２３】本発明の実施形態において、新規アプリケーションは公衆または専用の回線を通じてダウンロードされ、スマートカードのマイクロコンピュータにインストールされる。新規アプリケーションは、モニター・アプリケーションのセキュリティ・メカニズムを用いてインストールされ、新規アプリケーションはオペレーションキーを供給される。新規アプリケーションは、カード所有者情報および新規のデジタル証明も供給される。新規アプリケーションは、スマートカードのマイクロコンピュータのソフトウエア・レジストリへ、ソフトウエア・レジストリのオブジェクト指向クラスに従って登録される。スマートカード・レジストリのコピーは金融機関

の電子貸金庫に貯えられ、電子貸金庫は、新規アプリケーション用のオペレーショナルデータ(operational data)のコピーを用いて更新される。新規アプリケーションの少なくともひとつのオブジェクトは、他のアプリケーションの少なくともひとつのオブジェクトと、スマートカード上で選択的に共有され、この選択的共有は、新規アプリケーションによる限定的または非限定的な共有の一方かまたは両方である。

【００２４】本発明の更なる目的、利点、および新規な特徴は、一部は後に続く説明で述べられ、また一部は以下を精査するか、本発明を実施して学ぶことにより、この技術に精通する者にはより明らかになるであろう。

【００２５】

【詳細な説明】スマートカード技術は単一機能磁気的ストライプカードから進化したので、各カード技術のコストは、提供できる能力に比例する。例えば、種々のカード技術のおおよその推定コスト範囲は、単機能磁気的ストライプカードが約０．１５ドル／カード、単機能チップ・カードが約２．５０ドル、多重技術ハイブリッドカードが約３ドル／カード、スタティック多重機能チップ・カードが約４ドル、接触・非接触組合せ式カードが約７ドル／カードである。

【００２６】本発明の実施形態のための多重機能チップ・カードのおおよその推定コスト範囲は約９ドルである。１２ヶ月から１８ヵ月毎にチップ処理パワーが２倍になり、かつコストが半減する、と予測するムーアの法則（Moore's law）は、多重機能カードの需要が時間とともに上昇するので、対応するコストは、時間の経過とともに常に下がることを示している。

【００２７】本発明の実施形態において、業界間をまたぐ多重機能スマートカードは２つ以上のアプリケーションを扱かうことができ、カード発行後に新規アプリケーションのインストールをサポートできる。多重機能スマートカードのアプリケーション機能には、例えば、クレジット、デビット、ストアード・バリューのような支払い媒体が含まれる。多重機能スマートカードの他の機能には、例えば、ファシリティやネットワークへのアクセスのためのアクセスキー、個人プロフィール、身上調査(demographic)および好み、に関する情報を管理するための情報マネージャ、暗号化や認証を実行するための暗号エンジン、およびロイアリティプログラムとクーポン用のマーケティングツールが含まれる。

【００２８】本発明の実施形態において、アプリケーション機能の可能な組合せが与えられれば、多重機能スマートカードは実社会と仮想社会との間の橋渡しの役目を果たす。例えば、カード所有者は同じカードを使って、インターネット上でも販売店ＰＯＳ端末でも買物を行なえる。Ｊａｖａカード・プラットフォームのようなスマートカード・インフラ・プラットフォームは多重機能カード環境をサポートし、その環境は、オープンで、確実、多重機能であって、ダイナミックなダウンロードが可能であり、チップのプラットフォームに依存せず、そして、広範なプログラマのベースを持つ。

【００２９】本発明の実施形態において、多重機能および多重アプリケーション・スマートカードという用語は、異なるグループの人には異なる意味を持つことが注目される。その違いは、機能とアプリケーション間の違いとして表現される。機能は包括的コンセプトであり、他方、アプリケーションは特定の実施におけるコンセプトの実際の実現化である。例えば、電子財布(pures)またはストアード・バリューは機能であり、他方、例えば、ＶＩＳＡ ＣＡＳＨまたはＭＯＮＤＥＸの財布はアプリケーションである。両者間の対応は、多くのアプリケーションが電子財布の場合のように単一機能に分類され、多くの機能が単一アプリケーションで具体化されるという点で、多対多である。例えば、ＶｉｓａのＶＩＳアプリケーションは、クレジットとデビットの両機能から構成される。従って、多重機能スマートカードは、例えば、スマートカード機能の２つ以上、従って発行時にインストールされるか、または使用中にロードされる、アプリケーションの２つ以上を扱うのに必要な処理能力と記憶容量を備えたチップ・ベースのプラスチック・カードとして定義される。

【００３０】本発明の実施形態において、広範なプラットフォーム・ストラテジが端から端まで適用されて、カードから端末、そして最後にはサーバーへ、ソフトウエアのダウンロードとアップグレードが同時に行なえる。システムはフレキシブルな分散アーキテクチャを提供し、それによってインテリジェンスつまり処理能力は、システムのいたるところに分散される。例えば、アプリケーションの必要性やビジネス要件にもよるが、電子ワレット(electronic wallet)のような、端末からカードまたはサーバーへの、処理能力の移動が許される。そのような端から端までの見通し(perspective)により、セキュリティ、性能、相互運用性、および標準化のようなシステム全体の関心事は熟慮して解決される。

【００３１】本発明の実施形態において、業界固有のアプリケーション・テンプレートまたは包括的アプリケーション(generic application)は、特化されたアプリケーションを作るように考案されるか、または受継がれる。テンプレートは、再使用を容易にし、カスタム化を可能にし、相互運用性を促進する。標準と相互運用性は密接に絡んでいて、標準が相互運用を可能にする。この限りでは、ＥＭＶ標準の再活性化は既存のデビットとクレジットの機能にストアード・バリューを追加する。同様に、スマートカード能力を、セキュア・エレクトロニック・トランザクション（Secure Electronic Transaction（ＳＥＴ））へ取り入れたことにより、業界が進展するのに伴って、チップ電子コマースのビジョンを強固にした。

【００３２】本発明の実施形態において、例えば、カード・アプリケーション・プラットフォームの開発において主要な焦点である３つの分野がある。そのような分野のひとつは、ダイナミック・アプリケーションの確実なダウンロードであり、それは、例えば、カードが発行された後でスマートカード上にカード・アプリケーションを安全にインストールするためのポリシーとメカニズムを含む。他のそのような分野はオン・カードアプリケーション・インタラクションであり、それは、例えば、カード・アプリケーションが相互に発見し安全にインタラクトすることを可能にするメカニズムを含む。もうひとつの分野はオフ・カードでのアプリケーション・インタラクションであり、それは、例えば、オン・カードアプリケーションとオフ・カードアプリケーション間の確実なインタラクションをサポートするための、そして先進的なシステム管理をサポートするためのメカニズムを含む。

【００３３】本発明の実施形態において、ダイナミック多重機能チップ・カードは、新規アプリケーション発行後のダウンロードを容易にするオン・カード・インフラ・サポートを有する。カードが発行された後でカード・アプリケーションが追加または削除されるので、それはダイナミックであり、本発明の実施形態は、そのような操作を容易にするために端から端までのアーキテクチャを提供する。バンクカード(Bankcard)やシティカード(Citicard)のようなリレーションシップ・カードは伝統的に、例えばシティバンク(Citibank)のような金融機関の顧客へのサービスを拡大するための媒体であった。多重機能カードは、顧客との関係を広げて深めるための金融機関の包括的戦略の一部として、例えば、ストアード・バリュー（前払い）、デビット（現払い）、クレジット（後払い）、およびCiticard（ＡＴＭアクセス）を、業界をまたぐ他のサービスと統合するリレーションシップ・カードを金融機関に提供する。更に、Bankcard のようなクレジット機能をリレーションシップの一部として取入れることにより、金融機関は、金融サービスリレーションシップを、例えば、Bankcard用に広げつつ、自らのブランドのリーダーシップを維持する。

【００３４】本発明の実施形態において、多重機能スマートカードは、多重機能スマートカードの携帯性と移動性によって、任意のアクセスを可能にする。そのようなカードは、例えば、新しい販売モデルの必須の部分であり、インターネット、ＧＳＭフォン(GSM phone)、ケーブル、ＷｅｂＴＶのような様々な配信媒体のところで全ての販売チャネルにアクセスするのに使用される。そのような任意性により、多重機能スマートカードは、顧客が、何時何処でも、どんな装置を経由しても金融サービスを行なうことを可能にする。

【００３５】本発明の実施形態において、多重機能スマートカードは、コンシューマとビジネスのエレクトロニック・コマース（電子商取引）で、 Citibank のような金融機関のグローバルな地位を固め、それを最大限まで高める。というのも、金融機関のコアビジネスは、価値（バリュー）の移転つまりマネーの移動、およびクレジットまたはその関連サービスの拡大にあるからである。磁気的ストライプカードに固有なセキュリティの欠如とその結果としての詐欺の受け易さが、金融機関に毎年、何百万ドルも失わせている。不正な変更を防ぐハードウェア、そしてスマートカードのオン・カード・インフラ・サポートが、発行者とコンシューマのために等しくセキュリティを高め、そしてコスト節減を提供する。

【００３６】本発明の実施形態において、多重機能スマートカードにより提供される主たる恩恵は利便性である。そのようなカードはコンシューマに多大な価値（バリュー）を提供し、例えば、コンシューマが所持する現金を少なくでき、コンシューマは任意に金融や他のサービスに何時何処でも、どんな装置経由でもアクセスでき、コンシューマが個人情報をオーガナイズするのを支援する。そのようなカードがコンシューマに提供する別の恩恵は統合化である。コンシューマは、なにもかもが１ヵ所またはひとつのカードに結合されるアイデアに魅了される。統合によってコンシューマは、ウオレット（札入,wallets）に所持するカードを少なくすることができ、同じカードを使用して、一連のアプリケーションが実行できる。そのようなカードはまさに、究極的な薄いクライアントである。カード上に情報がますます統合されるにつれて、潜在的なカード紛失の問題が生じてくる。金融機関はコンシューマに、カード上のその貴重な情報をバックアップする手段を提供し、それによって金融機関を、独特なマーケット差別化地位に据えて、顧客との関係を更に強化する。

【００３７】本発明の実施形態において、そのようなカードにより顧客に与えられる更なる恩恵は情報の蓄積である。カード上に情報を蓄積するというコンセプトは、コンシューマへの強力な提案である。これは、書式に記入する場合のような時間の節約だけでなく、薬物に対するアレルギ、あるいは保険情報のような重要緊急時情報を蓄積する場合のような人命救助にも供し得る。そのようなカードにより顧客に与えられるなお更なる恩恵はカスタム化である。多重機能カード環境のダイナミックなダウンロード性により、コンシューマは、個人の要求と好みに基づいてアプリケーションを選択することにより、カードをカスタム化できる。これはカードのコントロールをコンシューマへ差し戻すことになり、カードはまさにコンシューマのパーソナリティやライフスタイルを反映するようになる。

【００３８】本発明の実施形態は、端末中心社会から、顧客中心のスマートカード中心社会へ移行させ、そこではスマートカードが究極的な薄いクライアントと見做される。スマートカードは、カード所有者が何時何処で

も、どんな装置経由でも、他の支払いやアクセスとともに、カード所有者がトランザクションを行なえるようにする、生体計測など、カード所有者のアイデンティティを保持する。そのような携帯性により、スマートカードは、現実と仮想の両方の世界を通じて、種々のサービスへの任意なアクセスが可能になる。

【００３９】本発明の実施形態において、相互運用性は、端から端までの異なるアーキテクチャーレベルで異なる意味を持つ。要するに、意味するところは、２つ以上のアプリケーションまたは参加者は、カード自体、カードとインタラクトする端末、カード・アプリケーションのための電子的カスタム化デポ(depot)、取得(acquisition)とカード管理システム、決済システム等のインフラのひとつひとつを使用できる。相互運用は多重機能カードを操作するのに必要な基礎であり、従って、エレクトロニック・コマース業界では多重機能スマートカードの非常に重要な特徴である。相互運用性は、あらゆるレベルで極めて重大な特徴であり、例えば、端末からカードへのインタラクションでのカード・アプリケーション中の、カード・インフラ内の所定の場所、そしてネットワーク・インフラ内の所定の場所にある。

【００４０】本発明の実施形態において、カード・インフラ・レベルで、システムは、標準化されたバーチャルマシン・インターフェースを持つとともに、Ｊａｖａカード・インフラにより提供されるようなサポート・クラス・ライブラリを持つ。カード・アプリケーション・レベルでは、業界内あるいは業界をまたぐ、異なるサービス・プロバイダからのアプリケーションが相互にインタラクトするようにするために、システムは、Ｊａｖａカード・インフラのようなカード・インフラ内に、および端末またはネットワーク・システムのところに、予め決められた１セットのインタラクションモデルを有している。端末レベルで、端末は、異なるアプリケーションを持つ異なるカードが２種類以上のタイプの読取られることができるほど十分にパワフルである。例えば、航空会社ロイヤリティ端末は、支払いを速くするようストアード・バリュー・カードを読取ることができ、かつセキュア・アクセス・アプリケーションは、電子チケットのゲート・アクセス環境で働く。ネットワーク・インフラ・レベルにおいて、ネットワーク・インフラは、複数のアプリケーション・メッセージング・スキームおよび／または通信プロトコル、そしてアプリケーションダウンロードをサポートする。

【００４１】本発明の実施形態において、Ｊａｖａカード・プラットフォームのようなカード・プラットフォームは、スマートカード・インフラの標準としての役目を果たす。Ｊａｖａカード・プラットフォームのようなカード・プラットフォームは、スマートカード用のインフラとして、カード上と端末の両方で、アプリケーションの相互運用を達成するように設計される。特に、Ｊａｖａカード用に設計されたスマートカード・アプリケーションは、Ｊａｖａバーチャルマシン（ＪＶＭ）とＪａｖａクラス・ライブラリをサポートする何れのカード上でも走ることができ、カードに追加できる。同様に、端末での相互運用は、その端末が、他端でＪａｖａカード・アプリケーションと交信能力のある低レベルのカード・エージェントまたはサービス・プロバイダを持っている時に達成される。そのような環境では、異なるベンダーが発行したカードは、種々の能力を持つ、何れのベンダーからの端末上でもシームレスに走る。

【００４２】本発明の実施形態において、金融サービス・アプリケーションは、例えばSchlumberger's Cyberflex カードを介して試作されたが、業界をまたぐアプリケーションは、Ｊａｖａカード２．０仕様のような次世代スマートカード・プラットフォームを利用している。このプラットフォームは、そのような多重機能カード環境の能力を立証するとともに、カード発行後どのように新規アプリケーションがカードに追加されるかを立証するのに使用する。カード・インフラを超えた先を見ると、アーキテクチャ上の革新が、端から端までの一貫したアプリケーション開発を可能にする。Ｊａｖａプラットフォームのような一連のプラットフォームは、異なるデリバリ装置とシステムを意図されていることがわかる。範囲を狭めると、そのようなＪａｖａプラットフォームは、例えば、Java JDK、personalJava、embedded Java、Java wallet、Java card、picoJava を含んでいる。

【００４３】本発明の実施形態において、テンプレートは、ストアード・バリュー、ロイヤリティ、または遠隔通信のような包括アプリケーションを定義するのに必須な、アプリケーションの基本的定義である。テンプレートは、金融機関の顧客に向けた特定の、ブランド付きアプリケーション・バージョンを構築することができる基礎である。テンプレートは、ブランド付アイデンティティではなくて、機能に関する。より技術的に言えば、テンプレートは包括アプリケーションを構築するための基礎を提供する。テンプレートは再使用を容易にし、従って、開発サイクルを短縮する。特殊化アプリケーションは、包括アプリケーションを基にして高めたものである。テンプレートは、ファイヤーウオールの対象になる、アプリケーション間の相互運用を容易にする。従って、例えば、ＭＡＳＴＥＲ ＣＡＲＤ／ＭＯＮＤＥＸ、ＶＩＳＡ、および ＥＵＲＯＰＡＹを横断して同一方法で働くベースライン・ストアード・バリュー・アプリケーションを持つことは有利である。

【００４４】本発明の実施形態において、業界固有のアプリケーション・テンプレートつまり包括アプリケーションは、特化アプリケーションを作成するために引出されるか、または受継がれて創られ、カード・アプリケーション・レベルで相互運用を達成する。カード・アプリ

ケーションの開発は、テンプレートを使用することにより調整される。テンプレートは再使用を容易にし、カスタム化を可能にし、相互運用性を促進する。プロセスを容易にするため、Smart Card Special Interest GroupsまたはＳＩＧ（業界セグメント毎にひとつ）が結成される。各ＳＩＧは、個々の業界のテンプレート開発に責任を持つ。この作業は、IATA Smart Card Subcommittee と Airline ICC を規定する IATA Resolution 791 の下でトラベル業界が行なう作業に類似している。

【００４５】本発明の実施形態において、標準と相互運用性は密接に関係していて、標準が相互運用を可能にする。この限りでは、ＥＭＶ標準が再度利用されて、既存のデビットとクレジットの機能へストアード・バリューを付加する。このことは、例えば、ＶＩＳＡ、ＰＲＯＴＯＮ、および他のストアード・バリュー製品が提供する機能をカバーする電子財布の統一定義に効力を与える。同様に、ＳＥＴ標準は、業界が進展するにつれて、チップ電子コマース(chip-electronic commerce)のビジョンを固めるよう、スマートカード能力を組み込んでいる。

【００４６】本発明の実施形態において、相互運用を容易にする他の標準は、例えば、 Microsoft のＰＣ／ＳＣとＮＣＩのオープンカード・フレームワーク（Open Card Framework（ＯＣＦ））である。最後に、金融機関は、次世代ＧＳＭとセット・トップ・ボックスのシステムに、ホームバンキングやエレクトロニック・コマースを含め、種々の金融サービスへ「任意」にアクセスするニーズを確実に含めるよう、遠隔通信とセット・トップ・ボックスの各業界と密接に作業を行なっている。これは、２－カードのシナリオを提供するセルフォンとセット・トップ・ボックスとにより実現されていて、そこでは、ユーザーがコントロールするスマートカードが、カスタム化アプリケーションに加え、確実なアイデンティティを提供する一方、特定の業界が発行した独立のカードが、基礎を成す遠隔通信またはインターネットサービスへのアクセスをコントロールしている。

【００４７】本発明の実施形態において、スマートカードは、エレクトロニック・コマース時代において現在そして将来見込まれる能力を持っている。しかし、インターネットとエレクトロニック・コマースの時代の技術マーケットは、セキュリティ上の脅威という問題に常にさらされている。購入注文と支払い認証との確実な交換を行なうために、公開キー・ベースの金融トランザクションが必須である。例えば、セキュア・エレクトロニック・トランザクション（ＳＥＴ）は、それ自体をエレクトロニック・コマースの世界の先導的標準と設定した。現在では、証明書(certificate)がＳＥＴプロセスの固有の部分である。それらはコンシューマ側のＰＣに格納される。セキュリティを別にすれば、携帯性または移動性の欠如がこのアプローチの欠点である。従って、例えば、自宅とオフィスでの使用のために別々の証明書を維持する必要がある。

【００４８】本発明の実施形態において、スマートカードに伴なう携帯性の懸念は、カードに証明書を設けることで解決される。証明書の所有、またはＥＭＶか提案しているようなある暗号が、カード所有者のＰＩＮを記憶するのと同じくらい容易になるように、現行の証明のサイズ（約１Ｋバイト）と、一連の証明のために認証プロセスを実行する必要性とから生じる困難は、カードの容量と業界標準が進化するとともに緩和される。代替として、証明書をＰＣに残したままで、ひとつまたはそれ以上のプライベートキーをカードに格納させることも当座の解決となる。

【００４９】本発明の実施形態において、確認することにより、カードは、カード所有者のアイデンティティと認証を唯一的に確認することができる。最も普通の確認メカニズムは、ＰＩＮを使用することである。しかし、ＰＩＮメカニズムは情報の秘匿性に基づいており、もしそれが失われたり、盗まれたり、あるいはカード所有者が忘れてしまうと、メカニズムは確実ではなくなる、つまりは信頼がおけなくなる。生体的測定を指向する確認は、ＰＩＮの負担もなく、高い精度と信頼性のある、所有者のアイデンティティを提供する。基準テンプレートつまりカード所有者の生体的測定のテンプレートは、ひとつまたはそれ以上の確認アルゴリズムとともにカードに格納され、人の個人識別標本がカードを離れることは決して無い。カード上でのテンプレート比較の代わりに、交換は、カードと端末間で確保される。加えて、２つの装置が相互に認証を行なって、秘密情報を保証されない環境へ曝露させる脅威を最少化する。

【００５０】本発明の実施形態において、スマートカードは、信用されるトランザクションのために、プライバシ、完全性、秘密性、非拒否性を提供する能力のある高性能マイクロプロセッサまたは暗号用コ・プロセッサを装備している。これは、暗号化（ＤＥＳ対称キーまたはＲＳＡ公開キーをベースとする）と認証（デジタル署名を比較する）を通じて遂行される。ＲＳＡ公開キー操作のような、時間がかかって計算の多い操作についての懸念を緩和するために、チャイニーズ・リマインダ法則（Chinese Remainder Theorem）（ＣＲＴ）のような技法を適用して、計算プロセスを更に加速する。代替として、楕円曲線暗号法（ＥＣＣ）も、短いキー長で同等のセキュリティを提供する。究極的には、旧い８ビットのスマートカード技術ではなく、例えば１６ビット、更には３２ビットのＲＩＳＣプロセッサを使用して、カード内からプライベートキーを創って、そのキーを使ってデジタル署名を生成することが好ましい。

【００５１】磁気的ストライプまたはパソコンに記憶された情報は、保証がなく容易に偽造または盗まれることが知られている。本発明の実施形態において、スマートカードは、物理的攻撃に対する耐改ざん性を提供するハ

ードウエア・トークンと見做される。加えて、情報は、カード上でファイルを読出したり、書込んだりするために、ＰＩＮ入力や生体的計測比較等、構成可能なアクセス・コントロール対策を通じて、未認証アクセスにするよう更に保護される。

【００５２】本発明の実施形態において、スマートカードは暗号化能力を持ち、暗号化するかまたはメッセージ認証コードを生成する（データをＭＡＣする）ことにより、カードと端末（またはホスト）間のメッセージ交換を確保する。データは、情報の更新または環境設定のためにカードへダウンロードされる。例えば、自らの電子チケットを使用する前に、遠隔サーバーへ一時的に格納しておくことを希望するカード所有者のために、短期間の記憶または長期間のバックアップ用に、サーバーへデータまたはトークン（代用貨幣）／チケットをアップロードを可能にする用意がなされている。更に、金融機関が、盗難または紛失カードを回復できるようにするために、顧客がカード上のデータをにバックアップする用意がなされている。

【００５３】本発明の実施形態において、スマートカードは、カードが発行された後に、新規アプリケーションをダウンロードする能力がある。これは、カードへの、およびカードからのデータの通常のアップロードをしのぐものであるとともに、カード所有者が、カードの機能を自らの好み合わせにカスタム化することを可能にする。Citibank のようなカード発行者のために、これは、例えば、ソフトウエアのアップグレード、新規アプリケーションの追加、そしてカード再発行を必要としないセキュリティ・アルゴリズム、の導入を可能にする。これは、所有することにかかるトータルコストの視点からは魅力的なビジネス提案である。

【００５４】本発明の実施形態においては、多くのカテゴリのカード・アプリケーションが提供されているが、それらは相互に排他的ではいない。単機能カード環境からダイナミック多重機能カードの世界に移行する中で、金融機関とコンシューマは、ひとつまたはそれ以上のカテゴリからアプリケーションを集合させることもできる。例えば、デビット、クレジット、ストアード・バリュー等の支払いアプリケーションは、ロイヤリティプログラム、ファシリティ・アクセス、およびネットワーク・アクセスのようなアプリケーションと並存できる。

【００５５】本発明の実施形態において、アプリケーションをグループに分類することは、個々のグループまたは業界内でアプリケーションを開発するためのフレームワークを確立するストラテジを形成する。例えば、情報マネージャグループは、包括的テンプレート、または、より正確には、例えば、プロフィール、人口動態、好みに関するアプリケーション等の特化アプリケーションを引出すために強化できる基本クラスと見做される。そのようなフレームワークの確立は、再使用を容易にしてカスタム化を可能にするのに利用される。関連アプリケーションにまたがる一体化インターフェースを確立する中で、電子的ワレットのようなオン・カードとオフ・カードの両アプリケーションのための、グループ化サービスへのアクセス性も最大化される。そのような設計原理は、追加の金融機関スマートカード発案のためにアプリケーションをオーガナイズする基礎を敷き、そして、アプリケーションの個々のカテゴリまたはクラスのためのインターフェース標準化へ向けて推進する。

【００５６】本発明の実施形態において、ストアード・バリュー・アプリケーションは、オフライン環境で現金の代替として、スマートカードは何を提供できるかという第一の考察を提示する。支払いアプリケーションは多重機能カード環境での要素である。統合された支払いカードは、全部で３種類の支払い方法、即ち、コンシューマ用のデビット、クレジット、およびストアード・バリューを含む。支払いカードは、エレクトロニック・コマース時代の実社会とバーチャル社会との間の橋渡しとしての役割を果たす。そのようなオープンの通貨支払いに加えて、他のクローズド・支払い媒体（バーター形式）は、例えば、電子チケットと通行トークン（システムへの支払いの形式として）、およびテーマパーク・トークン（GameWorks および Disneyland のような閉じたエンターテイメント環境で使用される）を含む。識別と確認のより強力な能力をてこにして、電子給付金（ペイメントの他の形）も同様に、スマートカードを通して支払われる。

【００５７】本発明の実施形態において、実社会またはバーチャル社会において安全で信用の有るトランザクションを行なうことは、例えば、２段階の確認と認証プロセスを必要とする。カード所有者のアイデンティティの確認、よおび、カードと、インタラクティング装置またはサーバーとの間の相互認証である。ＰＩＮ、または指紋のようなバイオ・テンプレートの形でカード所有者のアイデンティティを保持する際、スマートカードは、確認プロセスを実行または容易にすることにより、ファシリティとネットワークへ確実にアクセスする手段を提供する。前者は、テンプレート合致アルゴリズムが、例えば、局所での確認のためのカード上に在ることを必要とする。

【００５８】本発明の実施形態において、ひとたびカード所有者のアイデンティティが成功裏に確認されると、スマートカードは、信頼されるトランザクションを確保するよう、端末または遠隔サーバーと相互認証を行なう。そのような能力が与えられると、カードは、実社会でのファシリティ・アクセスのための、そしてバーチャル社会でのネットワーク・アクセスとＥ・コマース・トランザクションのための、両方のアクセスキーとして振舞う。包括的な暗号フレームワークが、暗号アプリケーション開発の基礎として確立される。そのようなフレー

ムワークは、そのようなサービスをオン・カードとオフ・カードの両方で使用できるようにして、再使用を最大にするとともに、マーケットへ出すまでの時間を短縮する。

【００５９】本発明の実施形態において、スマートカードは、カード所有者の価値（バリュー）と情報の両方を確実に格納することを基礎にして、例えば、銀行とその顧客間の信用関係を強化する。カード所有者に関する幾つかのタイプの情報をカードに格納できる。例えば、名前、血液型、誕生の日付と場所、母親の実家の姓、住所、電話番号のような個人情報を格納できる。婚姻状況、子供の数と年令、収入レベル、趣味等のプロフィールや人口動態情報も格納できる。更に、言語、頻繁にかける電話番号、航空機座席番号、コンピューター機器構成等の好みの情報をカードに格納できる。加えて、コンピュータとネットワークへのアクセスに関する所管地位のような権利や資格の情報をカードに格納できる。

【００６０】本発明の実施形態において、スマートカードは、カード所有者の個人情報を保護して管理する情報管理の役割を、カード所有者に代わって果たす。コンシューマのプライバシがスマートカードとエレクトロニック・コマース業界の主要な懸念であるので、これは重要である。異なる種類の情報は、アクセスを認可するために異なるレベルのセキュリティ対策が必要である。銀行のような金融機関とその顧客との信用関係の大きな部分は、金融機関が顧客の個人情報をどのように上手に管理するかにかかっている。フレキシブルであってもなお安全な情報アクセス・メカニズムが提供されており、医者のオフィスでの書式書込みに似たアプリケーションが、プライバシを侵害する懸念も無く自動化できる。

【００６１】本発明の実施形態において、スマートカードは、各小売店用のロイヤリティポイントまたはクーポンを格納することにより、販売店と金融機関の両方にマーケティング・ツールを提供する。オン・カード・ロイヤリティ・アプリケーションは、即時のロイヤリティポイントの報奨や割戻しを含むフレキシブルなショッピングでの特典を、カード所有者に提供する。加えて、教会や学校は、例えば、自らの販売に起因するものを益する仮証券(scrip)を発行することができる。

【００６２】本発明の実施形態において、カードが発行された後で新規アプリケーションをダウンロードできるようにすることにより、スマートカードは、カスタム化サービスを分配する際の独特のデリバリーチャネルを提供する。カード所有者は、自らのライフスタイルの進化とともに、カード上のアプリケーションを決めて、調整をすることができる。例えば、カード所有者は希にしか使わないアプリケーションを削除して新規のものを追加できる。セルフォン、セットトップ・ボックス、およびネットワークコンピュータのような多重のデリバリーチャネルと共に、パーソナル化能力が更に増幅される。コンシューマは、スマートカードを通して配送される金融トランザクションを実行したり、サービスを要請したりする際、追加の利便性とフレキシビリティを手に入れる。

【００６３】ここで、添付の図面に図解されている本発明の実施形態を詳細に参照すると、図１は、本発明の実施形態のための、アーキテクチャのシステム全体の主要構成要素の概観を示す。図１を参照すると、端から端までのアーキテクチャは、カード２から端末４へ、フロントーエンド・システム６へ、ネットワーク８へ、そして、最終的にはバックーエンド・サーバー１０までの諸問題と懸念を考慮に入れている。そのような端から端までのパースは、システムの重要な局面であり、セキュリティ、性能、相互運用性、標準化等のシステム全体にわたる懸念を反映し解決することを可能にする。この多重機能世界では、カードに必要な性能とセキュリティを測るために、そのような理解を持つことが是非とも必要である。これは、端末４とバック・エンド・サーバー１０との間と同様に、カード２と端末４との間の相互運用性と標準化の懸念を解決することもできる。例えば、このシステム・アーキテクチャは、一端で破壊されたセキュリティが、他端から回復されるように、あるいは最小限になるように設計されている。

【００６４】更に図１を参照すると、端から端までのアーキテクチャの５つの主要構成要素には、例えば、スマートカード２、端末４、フロントーエンド６、ネットワーク８、および、バック・エンド・サーバー１０がある。カード発行者は、カード２とバック・エンド・サーバー１０の両方でセキュリティ対策を全面的にコントロールする。端末４および６とネットワーク８との間は安全ではないとみなされ、特別な注意をもって扱われる。他方、インテリジェンスと処理能力はシステム全体に分散されている。アプリケーションのニーズに依存して、インテリジェンスは、カード２から端末４へ、そしてサーバー１０へ伝達され、またはその逆に伝達される。

【００６５】本発明の実施形態において、究極的な薄いクライアントとして振舞うスマートカード２は、銀行のような金融機関とその顧客との間の信用関係を更にてこ入れしたリレーションシップ・カードである。これを遂行するために、カード・インフラは、必要な多重機能性とダウンロード能力をサポートする。そのようなプラットフォームの例がＪａｖａカードであり、バーチャル・マシンとサポーティング・クラス・ライブラリを包含する。図２は、本発明の実施形態のための、カード・プラットフォームにおける階層段階のサンプルを示すチャートである。Ｊａｖａカード・プラットフォームのようなカード・プラットフォームは、そのアーキテクチャ内に階層段階を提供する。例えば、Mondex のMULTOSの場合のように、Ｊａｖａカード・バーチャル・マシン（ＪＶＭ）１６は、専有かオープンのいずれか一方のカ

ード・オペレーティング・システム１４の上に載っている。

【００６６】本発明の実施形態での、アプレットという用語は、サイズがコンパクトで公衆回線上へダウンロード可能であるスマートカード・アプリケーションを意味する。図２を参照すると、ＪＶＭ１６のようなカード・アーキテクチャは、未認証のアプレットがカード上で実行されるのを防ぐためにバイトコード認証(bytecodeverification)を提供することにより、実行中に追加セキュリティを提供する。バイトコードはマシンに依存せず、ＪＶＭ１６により解釈される。ＪＶＭ層１６の上にあるのは、基礎クラス・ライブラリ１８であり、Ｊａｖａカード・アプリケーションを構築するインターフェースを提供する。フレームワークをベースにしたそのようなアプローチは、アプリケーション開発での再使用を容易にするとともに、マーケットへ出すまでの時間を早めることができる。そのビジョンを更に拡張するために、業界固有のおよびアプリケーション固有のテンプレート２０が創り出され、それは、特化されたアプリケーションを生じるように引出されまたは受継がれる基礎クラス・ライブラリである。かくして、相互運用がカード・アプリケーション・レベルで達成される。最後に、階層のトップには、カード２上に調和して併存する一連の、業界をまたぐアプリケーション２２がある。

【００６７】本発明の実施形態において、種々の端末とアクセス装置４は、スマートカード・インターフェースを持つ。これらはＡＴＭ、ＰＯＳ端末、（スタンドアロンまたはキーボードの一部に）スマートカード読取装置を有するＰＣ、個人用情報機器（ＰＤＡ）、セット・トップ・ボックス、セルフォン、ケーブル／衛星ＴＶ受像機、各種の接触／非接触式読取装置を含む。デザインは、カードと端末の両方のアプリケーションが、同時にアップグレードされてシームレスな移動が可能になるように、カード２と端末４との間の一体のアーキテクチャを提供する。例えば、ＰＣ上に在るか、またはネットワーク上に分散する電子ワレットは、支払いサービスおよび情報管理をインターネット上で配送する媒体を提供する。スマートカード２は、ワレットを自然的に拡張したものであり、ワレットの機能性の幾分かを物理的に含む。スマートカード２はワレットの物理的実物として進化する。このように、ワレットの機能性の特定の一部分はカード２に移され、一方で他は端末４またはブラウザ上に留まるか、またはサーバーへ移る。ネットワーク上でのインテリジェンスの分散は、このような移動形式で実現される。

【００６８】本発明の実施形態において、アーキテクチャの視点からは、ワレットのデータは物理的に、例えば、カード２または遠隔サーバー上に在る。格納場所は情報の性質とカード２の容量制限に基いて編成される。物理的な場所に拘らず、ユーザーは情報へ容易にアクセス可能である。ユーザーが、トランザクション中に適切な決定をするようデータのある実際の場所を意識的に理解したいと希望する状況では、スマートカード・アーキテクチャがそのような決定プロセスを容易にする。サーバー上に重要な情報を格納するかまたはバックアップすることはカード所有者の貴重な情報を保護する強力なメカニズムである。

【００６９】本発明の実施形態において、カード２が紛失したり盗まれた場合、金融機関は新規のカードを確信を持って金融機関のサーバーから回復したオリジナルのカード情報（格納されたバリューではない）を搭載し発行する。この回復性をもって、金融機関の顧客は、信用される金融機関が彼らのために情報を確保していることを知り、安心する。これは、言換えれば、銀行のような金融機関にマーケット差別化を提供する、それはカードを紛失することがコンシューマの懸念トップのひとつになるからである。生体測定ベースの確認を可能にするため、指紋または手の形状寸法（ジオメトリ）用スキャナーのような生体測定スキャニング装置が端末４に搭載される。捕捉されたデータはカード４上の基準テンプレートと照合され、カード所有者が真正であることを確認する。

【００７０】本発明の実施形態において、フロント・エンド・システム６は、端末４に至るフロント・エンドとして利用する。その原則的な責務は、端末４とバック・エンド・サーバー１０間のメッセージ・プロトコルの必要な翻訳を提供することである。それは、スマートカードを扱える端末４がバック・エンド・レガシー・システム(back-end legacy system)１０に対しトランスペアレントであるように、ネットワーク化環境でミドルウエアまたはゲートウエイの役割をはたすことが多い。ネットワーク８は分散環境でのプラミングを行なう。システムでは公衆（オープン）と私用（専用）両方の回線が使用される。前者には、例えば、インターネット、ＰＬＵＳ、Ｃｉｒｒｕｓ、Ｓｔａｒを含み、後者は、例えば、Ｃｉｔｉｓｈａｒｅが含まれる。

【００７１】本発明の実施形態において、金融サービス環境では、バック・エンド・サーバー１０が清算と決済の機能を扱う。幾つかのバック・エンド・サービスは、証明機関（Certificate Authority）（ＣＡ）、電子カスタム化デポ(Electronic Customization Depot)（ＥＣＤ）、電子貸金庫(Electronic Deposit Box)（ＥＤＢ）、電子金庫(Electronic Vault)（ＥＶ）等のダイナミック多重機能環境での、オペレーションをサポートする。金融機関は、マーケットの差別化と顧客との更なる関係に備えるために、ひとつ以上のそのようなサービスを提供することができる。特定のサービスはそれらの機能に従い論理的に考案される。二種類以上のサービスを、ビジネスのニーズとデザイン決めに従って、同一のサーバー１０へ物理的に存在させることができる。

【００７２】本発明の実施形態において、証明機関（ＣＡ）は信任を受けたた第３者である。この機関は顧客、販売店、およびインターネット上で公開キーベースのトランザクションを行ないたい人に、証明書を発行する責任を負う。セキュア・エレクトロニック・トランザクション（ＳＥＴ）オペレーションは証明ベースである。このように、ＣＡは、本来的にセキュア・トランザクション・プロセスの何れにも不可欠な一部分となる。金融機関は、自らの顧客とのインタラクションの最大化を目的とするＣＡとなり得る。

【００７３】本発明の実施形態において、電子カスタム化デポは、アプレットを追加したり削除したりして、顧客のカードをカスタム化するオプションを顧客に提供するアプレット・サーバーおよびモニター・アプリケーション・サーバーとして振舞う。アプレット・サーバーとしては、それはアプレットのダウンロード用、およびカードの回復用のソースである。各モニター・アプリケーションは、顧客のスマートカード２へアプレットを確実にダウンロードする責務を負う。ロードキーは、例えば、操作を容易にするようモニター・アプリケーションに格納される。実社会での貸し金庫や金庫に相当するものは、バーチャル世界の電子貸金庫と電子金庫である。顧客の貴重品を信頼できる確実な環境に保管するのが目的である貸し金庫と同様に、電子貸金庫は金融機関の顧客に同様なサービスを提供する。

【００７４】本発明の実施形態において、顧客の要求があると、金融機関は、顧客のスマートカード上の貴重情報を格納するか、あるいはバックアップする。電子貸金庫はひとまとめにして、電子金庫に集合される。電子トークンや電子チケットを含めて、顧客の貴重な情報を保持することに加え、個々の電子貸金庫は各顧客のカード２のソフトウエア在庫も維持している。そのような在庫を用いて、金融機関は、カードが紛失または盗まれた時、顧客のために、例えば、電子カスタム化デポからカード・アプリケーションを回復することができる。

【００７５】本発明の実施形態において、ダイナミック・アプリケーション・ダウンロードのようなアプリケーションをサポートするために、ファシリティが提供されており、このファシリティは、カードが発行された後、スマートカード２上にカード・アプリケーションを確実にインストールするのに必要なポリシーとメカニズムである。他のそのようなファシリティは、オン・カード・アプリケーション・インタラクションを含み、これは、カード・アプリケーションが相互に発見し、安全にインタラクションすることを可能にするメカニズムである。追加のそのようなファシリティは、オン・カード・アプリケーションとオフ・カード・アプリケーションとの間の確実なインタラクションと、先進的システム管理とをサポートするメカニズムのようなオフ・カード・アプリケーション・インタラクションを含む。オン・カード・

アプリケーションはアプレットと呼ばれることが多い。必要に応じ、スマートカード２へインストールされたアプリケーションは、デスクトップ、端末、またはメインフレームの各アプリケーションに比較すると、非常に小さい傾向があり、従がって、それらはアプレットと称される。

【００７６】本発明の実施形態において、スマートカード・アプリケーション・プラットフォームは、２つの全体的セキュリティ目標を満たす、すなわち、カードのシステム構成要素の、セキュリティと完全性を確保すること、そして、拡張性のあるメカニズムを有するアプレットを提供して，それら自らのセキュリティと完全性とを確保することである。カード２に対する全体的セキュリティ・ポリシーは、認証されたエンティティだけがカード資源にアクセスを許され、そしてこのアクセスは、アクセスが承諾されている活動に限られる。金融機関のセキュリティ目標が満たされることを確保するために、カード・アプリケーション・プラットフォームは幾つかの重要な要素を含み、うち２つが、マスター・アプリケーションとモニター・アプリケーションである。特殊なシステム・アプレットとして、マスター・アプリケーションがカード発行者を代表する。それはグローバル・カード・サービスを提供し、例えば、カード２にアプレットをインストールすること、グローバル・データをパーソナル化するとともに読出すこと、カードのライフ・サイクル状況を管理すること、カードがブロックされた時に外部監査をサポートすること、各アプレットに関連付けられたモニター・アプリケーションのマップを維持することを含む。

【００７７】本発明の実施形態において、システムは、他のアプレット・プロバイダにより開発されたアプレットと、金融機関自身のアプレットとを含む。このように、カード・アプリケーション・プラットフォームは、多数のプロバイダからのアプレットの確実でしかも秘密のインストールをサポートする。アプレットの、確実なインストールをサポートするために、金融機関はモニター・アプリケーションを使用する。モニター・アプリケーションは、アプレット・プロバイダにより供給される特殊なアプレットである。各モニター・アプリケーションは、プロバイダのひとつまたは複数のアプレットのインストールをコントロールする。カード上には多数のモニター・アプリケーションがあり得る。各モニター・アプリケーションは、単一のアプレット・プロバイダのために唯一の暗号関係を表現する。暗号メカニズムとキーから成るそれの唯一の組合せを使用して、各モニター・アプリケーションは、カード２にロードされたアプレットの署名チェックと暗号解読を管理する。従って、カード２上のモニター・アプリケーションをインストールし初期化することは、プロバイダのアプレットの確実なダウンロードをサポートするために必須なステップであ

る。

【0078】本発明の実施形態の別の重要な側面はカード2上へのマスター・アプリケーションのインストールであり、それはモニター・アプリケーションと連結して機能する。マスター・アプリケーションは、例えば、スマートカード2上で、アービター、ゲートキーパー、メッセージ・デスパッチャとして使用する。カード上でのアプリケーションからアプリケーションへの直接のインタラクションは許されない。その代わり、全てのインタラクションは、スマートカード2上で、アービター、ゲートキーパー、メッセージ・デスパッチャとして使用するマスター・アプリケーションを通さねばならない。マスター・アプリケーションは、アプリケーション間の交信中、アービターとして働らく。ひとつのアプリケーションが発動するどのようなリクエストも、例えば、偽リクエストを防止する予備チェックのために、それが目的地であるアプリケーションに至る経路が見い出される前に、マスター・アプリケーションへ送られる。そのようなリクエストは、例えばファイル・アクセスまたはサービス解釈であり得る。いずれの場合でも、リクエストを引受けるかどうかは、目的地または受け手のアプリケーションが決めることである。

【0079】マスター・アプリケーションがゲートキーパーの役をするのは、例えば、ダイナミック・アプリケーションのダウンロード中にカード2上へ未認証のアプリケーションがダウンロードされるのを防止するためである。そのような能力で、マスター・アプリケーションは、個々のモニター・アプリケーションと連結して動作して、必要な認証と有効化の機能を実行することにより、ダウンロードされたアプリケーションが合法的なソースから来たこと、そしてその内容が変更されてはいないことを保証する。

【0080】マスター・アプリケーションは、例えば、端末からカードへのインタラクション中はメッセージ・デスパッチャとして使用する。メッセージ・デスパッチ・プロセスは簡易であるが、強固な、メッセージ・ルーティングメカニズムであり、ほとんどオーバーヘッドを受けずに、メッセージのタイムリなデリバリを保証する。到来する各メッセージは、順次、カード2に在る各アプリケーションへルーティングされ、そして、そのような各アプリケーションは、それが、メッセージの、意図された受取人であるか否か判断する。もしそうであれば、特定のアプリケーションがそのメッセージを処理し、「成功(success)」回答を返す。そうでない場合、アプリケーションは「エラー(error)」メッセージを返し、マスター・アプリケーションは、「成功」回答が返ってくるまで、カード2上の他のアプリケーションへメッセージを送り続ける。その後、特定のアプリケーションが「エラー」メッセージを返すまで、次のメッセージが最後に成功したアプリケーションへ送られ、このサイクルが繰返される。

【0081】本発明の実施形態のもうひとつの重要な局面は、カード2上に統合された識別アプリケーション（IDアプリケーション）のインストールである。IDアプリケーションは、データの重複を避けるために、全ての個人プロフィール関連情報用の単一プレースホルダ（place holder）として使用する。あるアプリケーションが識別関連情報を必要とする時、そのアプリケーションは自らの識別と許可レベルを提出する、そして、IDアプリケーションは、データ・アクセスをリクエストしているアプリケーションに与えられる特権がもしあれば、それを決定する。例えば、健康管理アプリケーションは、カード所有者の血液型情報にアクセスできるが、ロイヤリティプログラムにアクセスすることはできない。

【0082】本発明の実施形態において、モニター・アプリケーションのインストールと初期化は、カードの初期化中に行なわれる。しかし、フレキシビリティを最大限にするために、金融機関は、カード2が発行された後、新規のモニター・アプリケーションのダウンロードとインストールをサポートする。この特徴をサポートするために、ルート・モニター・アプリケーションが、カードの初期化とパーソナル化中にインストールされる。引き続き、ダウンロードされた各モニター・アプリケーションは、金融機関が特定アプレットをダウンロードしインストールすることを可能にする。アプレットの実際のダウンロードとインストールが行なわれる前に、適切なモニター・アプリケーションがアプレットのダウンロードを認証する。従って、アプレットがダウンロードされる前に、アプレットを識別するアプリケーション識別子（AID）が、識別されたアプレットのダウンロードを認証できるように、適切なモニター・アプリケーションにより登録されねばならない。

【0083】図3は、図1に示される情報の流れを強調した概略線図であり、本発明の実施形態のための、アプレットを選択し、スマートカード2へ確実にダウンロードするプロセスに関する更なる詳細を提供する。図4は、本発明の実施形態のためのアプレットを選択しスマートカード2へ確実にダウンロードするプロセスに関する更なる詳細を提供するフローチャートである。S1で、スマートカード2は、PINまたは、指紋のような生体的計測を有するカード所有者24のアイデンティティを確認するアプレットを含む。S2で、システムにより提供されたサービスの選択オプションから、カード所有者24が、オプションを選択して新規アプレットをダウンロードする。カード2とカード所有者24は両方とも、システムがダウンロードのための何らかのアプレットを提示する前に、資格が与えられねばならない。S3で、カード所有者24とひとつ以上の関係をベースにしたビジネスによりサポートされたアプレット、およびカ

ード2上で利用できるスペースに合うであろうアプレットをシステムが提示する。

【0084】本発明の実施形態において、アプレットに課せられたスペース資格付与は、各アプレットが依存する他の何れのアプレットも含め、各アプレットが必要とする全スペースを明らかにしなくてはならないことは注目される。かくして、アプレットは、クラスタにグルーブ化されてもよい。それで、もしひとつのアプレットが、カード2上に未だインストールされていない他のアプレットに依存していれば、カードは、そのような依存クラスタを形成する全てのアプレットを収納するのに十分なスペースを持つ。S4で、システムは、例えば、アプレットのプロバイダを識別するのを助けるブランドを含む、有資格のアプレットのリストをカード所有者24に提示する。アプレット選択中にカード所有者24がインフォームド・デシジョンを行なえるようにする幾つかの種類の開示がある。代表的ないくつかの例は、各アプレットの全体サイズ、カード2上の利用可能スペース、カード・インフラで固有なその他の制限がある。例えば、一旦アプレットがインストールされると、それは動かせないし、割当てたスペースは回復できない。

【0085】本発明の実施形態において、S5で、カード所有者24は、提供されたアプレット・リストからひとつのアプレットを選択する。S6で、選択されたアプレット用のモニター・アプリケーションがカード2上に存在しない場合、新規アプレットが電子カスタム化デポ内のアプレット・サーバーからダウンロードされる。S7で、新規モニター・アプリケーションがカードに追加された場合、その新規モニター・アプリケーションは、電子的カスタム化デポ内のセキュリティ・サーバーから得られる何れかひとつまたは複数の必要キーで初期化される。S8で、モニター・アプリケーションが提供するセキュリティ・メカニズムと、例えば、モニター・アプリケーションのゲートキーパー機能とを使用して、選択されたアプレットが電子的カスタム化デポ26内のアプレット・サーバーからダウンロードされてインストールされる。S9で、電子的カスタム化デポ26内のセキュリティ・サーバーは、その操作に必要なひとつまたは複数のキー付きの新規アプレットを供給する。

【0086】本発明の実施形態において、アプレットが何らかの顧客情報を要求する場合、それは顧客リレーションシップ・ファシリティ28から得られる。アプレットがデジタル証明書を要求する場合、それは適正な証明機関30から得られる。S10で、カード所有者リレーションシップがそれをサポートする場合、新規アプレットはカードのソフトウエア在庫に登録される。カード・ソフトウエア在庫のコピーは銀行の電子金庫32内の、カード所有者の電子貸金庫に維持される。加えて、カード所有者の電子貸金庫は、たとえあったにしても、カード紛失時に再発行されるキーや証明書を使うのではなく、アプレットのオペレーショナルデータのコピーを使って更新される。

【0087】本発明の実施形態において、確実で信用される環境を創るために、アプレットは相互に隔離される。アプレット・ファイアウオールは、ひとつのアプレットが、他のアプレットの所有するオブジェクトの内容と振舞いにアクセスすることを防ぐ。しかし、中には、信用のある方法で相互に交信できるアプレットがある。Ｊａｖａカードのようなスマートカードは、アプレット間でオブジェクトを明白に共有するための2つの基本メカニズムを提供する。そのようなメカニズムのひとつは限定的共有であり、もうひとつは非限定的共有である。限定的共有は、ひとつのアプレットが、共有されたオブジェクトへの特定の他のアプレットによるアクセスを許す。非限定的共有は、ひとつのアプレットが、共有されたオブジェクトへの他の全てのアプレットによるアクセスを許す。この2つの基本メカニズムを組合せて使用し、選択的なオブジェクト共有を実行する。選択された情報とサービスを共有するいくつかのアプレットがある。例えば、支払いアプレットは、ロイヤリティ・アプレットとのインタラクションにより、支払いトランザクションの一部としてロイヤリティポイントを追加する。しかし、ロイヤリティ・アプレット・プロバイダは、特定のプロバイダからのアプレット、または特定の種類のペイメント・アプレットにこのインタラクションを限定することができる。この種の選択的相互運用性をサポートするために、アプレットのうちのあるものは、共有されたオブジェクト登録のためのメカニズムを持つ。

【0088】本発明の実施形態において、アプレットは、カードが発行された後、カード2上にダウンロードされてインストールされることができる。従がって、既にカード2上に存在するアプレットは、新規アプレットが予め存在するアプレットとともに、自らを登録するまでは、新規にインストールされるアプレットに関する知識は持っていない。一旦、新規アプレットが予め存在するアプレットに対して自らを同定すると、予め存在するアプレットは、新規アプレットがその共有されたひとつまたは複数のオブジェクトへアクセスすることを許諾できる。このように、予め存在するアプレットまたは共有アプレットは、その共有されたひとつまたは複数のオブジェクトのために、他のアプレットの登録をサポートする。

【0089】本発明の実施形態において、共有されたオブジェクトの登録を推進するために、共有アプレットは、資源ガーディアン（guardian）への非限定的アクセスを許諾する。資源ガーディアンは、共有アプレットの共有されたひとつまたは複数のオブジェクトと呼ばれる保護された（guard）あるひとつまたは複数の資源への限定的アクセスをコントロールし許諾する。アプレットのあるものは、幾つかの種類のアプレットが使用するの

に十分包括的な、再使用できる基礎クラス・ライブラリ、またはＪａｖａクラスのグループを含む。あるオブジェクトの使用に対するコントロールを維持し、それによって信用を維持するために、これらのライブラリのあるものは共有されたオブジェクト・ファクトリを含む。共有されたオブジェクト・ファクトリは、特定クライアント・アプレットのリクエスト時、ライブラリ・クラスの新しい実例を創り、クライアントアプレットによるアクセスのためにその新しい実例を登録する。

【００９０】本発明の実施形態において、あるアプレットは情報とサービスを共有する。しかし、カード所有者２４に、アプレットを選択しダイナミックダウンロードする能力を与えることは、アプレットが、カード２に予め定められた順序ではインストールされ得ないことを暗示する。例えば、ロイヤリティアプレットは、幾つかの種類の支払いメカニズムとのインタラクションをサポートするように設計されることができる。新規支払いメカニズムがカード２にインストールされた時、互換性のある何らかのロイヤリティアプレットが既にカード上にあるか否かを発見したいと望むであろう。従がって、ダイナミックにアップロードされたアプレットがインストール中にどのような他のアプレットがカード２上に存在するかを発見できるようにするために、カード・アプリケーション・プラットフォームはアプリケーション・レジストリを含む。

【００９１】本発明の実施形態において、アプリケーション・レジストリは、自らの識別に基づくアプリケーションと、自らの機能性またはオブジェクト指向分類に基づくアプリケーションとの間の連鎖をサポートする共有されたオブジェクト登録メカニズムを提供する。このように、新しくインストールされたアプレットは、ＡＩＤを使用してカード２上にもうひとつのアプレットが存在するか否かを発見することができ、また、特定の機能的インターフェースを実行するか、または特定ベース・クラスから引出された他の何れかのアプレットがカード２上に存在するか否かを発見することができる。

【００９２】本発明の実施形態において、アプレットが相互に自らの機能性に基づき発見またはリンクするのを可能にすることは、単独的な識別に対してはるかにフレキシブルな代替を与える。このことは、それらがスマートカード２上での多重機能の単純な散開を超えて多重機能的統合のレベルを達成することを可能にする。または、端末が、実際にカード上に存在するアプリケーションによりサポートされた機能性に基づき、ダイナミックにかつインテリジェントにカード２とのインタラクションに端末を適合させることも可能にする。オン・カード・インタラクションをサポートするファシリティに加え、カード・アプリケーションは、カード端末４またはバック・エンド・システム１０のどちらに在住しても、オフ・カード・アプリケーションとのインタラクションを容易にするサービスを持っている。

【００９３】本発明の実施形態において、ダイナミックなアプリケーション・ダウンロードに関連するセキュリティ・メカニズムは、一方向にだけ適用されるという点で非対称である。ダウンロードされたアプレットは暗号を解読され、カード２へインストールされる前に、完全性と真実性が確認される。しかし、アプレット自体は、セキュリティのために対称メカニズムを持つ。それらは、例えば、データの暗号化と解読、デジタル署名の生成と確認、メッセージ認証コード（message authentification code）（ＭＡＣ）の生成と確認のためのサポートを持つ。カード・アプリケーション・プラットフォームは、キー生成とキー管理用のサービスを含む、一体で、一貫する、対称使用とともに、多様なセキュリティ・メカニズムを一括することをサポートする暗号基礎クラスのようなファシリティを含む。

【００９４】本発明の実施形態において、カード所有者２４がますます多くの種類の情報をカード２上に詰め込むにつれ、カード所有者に対するカードの価値（バリュー）は当然ながら増加する。かくして、カード２の紛失は、カード所有者２４にとって相当な損失となる。この損失の重要性を減少させるべく、システムは、カードが紛失した場合にそれを再発行するために、カード２上に含まれる情報を回復するメカニズムを提供する。金融機関は、各々のカード所有者２４のために電子貸金庫を含む確実なオフ・カード情報格納ファシリティつまり電子金庫３２を提供する。各々の電子貸金庫は、インストールされた各アプレットが管理する情報のコピーと同様に、カード２上へインストールされたアプレットのソフトウエア在庫を含む、カード所有者２４が銀行に登録した各カードの内容のコピーを含む。

【００９５】本発明の実施形態において、金融機関以外のプロバイダのアプレットを、カード２へインストールできる。そのような他のアプレットのプロバイダは、それらのアプレットが管理するセキュリティ・キーおよびデータの保護に合法的な関心を持つ。アプレットのデータ回復をサポートするために、カード２上のアプレットと電子金庫３２は、データ交換のために確実なプロトコルを使用することにより協働する。アプレット・プロバイダの秘密性をサポートするために、各アプレットは暗号化を利用して、電子金庫３２内のコピーされたデータが調べられることを防ぐ。これらの電子的セキュリティ・メカニズムはともに、貸金庫に貴重品を保管するのに使用される物理的なセキュリティ・メカニズムを模倣する。例えば、貸し金庫に保管された貴重品にアクセスするには２つのキーを必要とし、そのひとつは顧客が所有し、もうひとつは銀行が所有する。このように、対称メカニズムを使用して、各アプレットはバックアップ中にその情報のブラインド・コピーを作製し、そして回復中にブラインド・コピーを使うことができる。電子金庫３

2は、各アプレットの情報のブラインド・コピーを保管する。

【００９６】本発明の実施形態において、スマートカード2は、クライエント－サーバー・アーキテクチャ内でサービス・プロバイダの役割を果たすことに限定されず、そこでは、カード2と端末4との間のインタラクションが、応答装置としてのカードとともに端末により開始されるが、システムはスマートカードを含むよりフレキシブルなアーキテクチャ・ソリューションを提供する。例えば、オン・カード・オブジェクトは、分散コンピューティング環境に関係して、離れた、オフ・カード・オブジェクトとのインタラクションを開始することができ、これは、例えば、遠隔呼出し法 remote method invocation（ＲＭＩ）のためのＪａｖａファシリティを含んで、Ｊａｖａカードのようなカード・プラットフォームによりサポートされる。

【００９７】本発明の実施形態において、分散オブジェクトに関係して、メカニズムはシステムによって提供され、トランスペアレント・オブジェクト分散をサポートする。このように、オン・カード・オブジェクトはそれらの位置の明白な知識無しにオフ・カード・オブジェクトと、またはその逆に、インタラクションできる。そのようなトランスペアレント性は、システム設計を単純化し、オブジェクトの所在を突き止めるのにより大きなフレキシビリティを可能にし、そして、電子金庫３２のようなひとつの場所から、カード2のような他の場所へ移動し得る、移動オブジェクトの展開をサポートする。例えば、電子チケットが購入され、そしてそれを使用する必要がある時、オフ・ライン受け戻しできるようスマートカード2上へ移動され得るまで、電子金庫３２に保管されることができる。

【００９８】本発明の実施形態において、展開されたアプレットの置換はＪａｖａカードのようなカード・プラットフォームがサポートする。アプリケーション識別子（ＡＩＤ）が割当てられ管理される。アプレットＡＩＤは、新規のアプレット・バージョンを展開する時に変更されることなく再使用される。その代わりに、余り望ましくはないが、唯一性を保証するためにバージョン識別子を含むＡＩＤ用のネーミング・スキーム（naming scheme）がある。メカニズムは、例えば、アプレット・クラスのあるものが自ら形を変更した時、アプレットのために創られたオブジェクトを置き換える。カードとオン・カード変更は困難または不可能であり、カードには制約が付与される。この要件はバックアップファシリティとしての電子金庫３２の価値を強める。

【００９９】本発明の実施形態において、アプレットの古いバージョンは、その全てのオブジェクトを含めて、完全に取り除くこともでき、そして新しいバージョン、および電子金庫３２で変更されたバックアップ・コピーから回復されたアプレット・オブジェクトとに置き換えられる。アプレット開発のためのクリーンルーム・ソフトウエア・エンジニヤリング・アプローチは、ソフトウエア開発プロセスに厳格なプロセス・コントロールを適用し、６シグマ品質のような極めて高品質のソフトウエアを作製する。スマートカードの資源が限られていることは、アプレットが比較的に小さく簡単であることを必要とする。このように、クリーンルーム・アプローチの厳格なプロセス要件は、大きなソフトウエア・プロジェクトに関するようには煩わしくはない。

【０１００】本発明の種々の好ましい実施形態が、発明の種々の目的の実現の中で証明されてきた。これらの実施形態は、本発明の原理の単なる実例であると認識されるべきである。この技術に精通する者には、本発明の精神と範囲から外れることなく、それらの多数の変形や改作が容易であることは明白であろう。従って、本発明は以下の特許請求項によってのみ限定される。

【図面の簡単な説明】

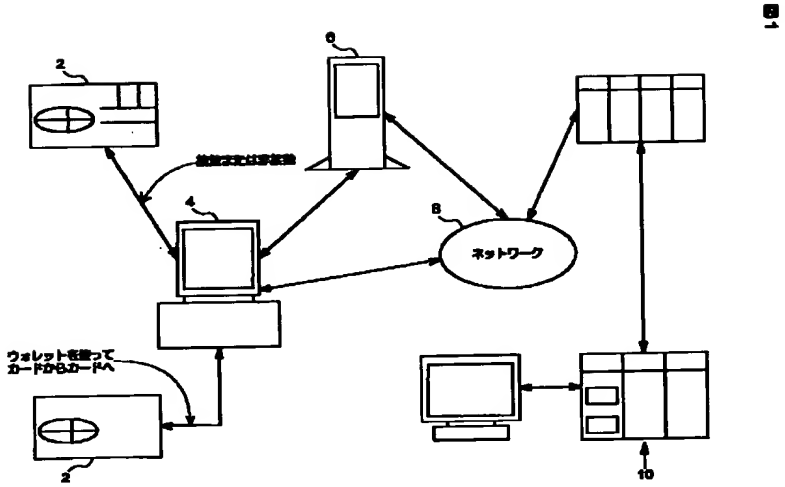
【図１】本発明の実施形態のための、主要構成要素の実施例の概観例と、システムの主要構成要素間の情報の流れを示す概略ダイアグラムであり、

【図２】本発明の実施形態のためのスマートカード・プラットフォームにおける階層構造のサンプルを示すチャートであり、

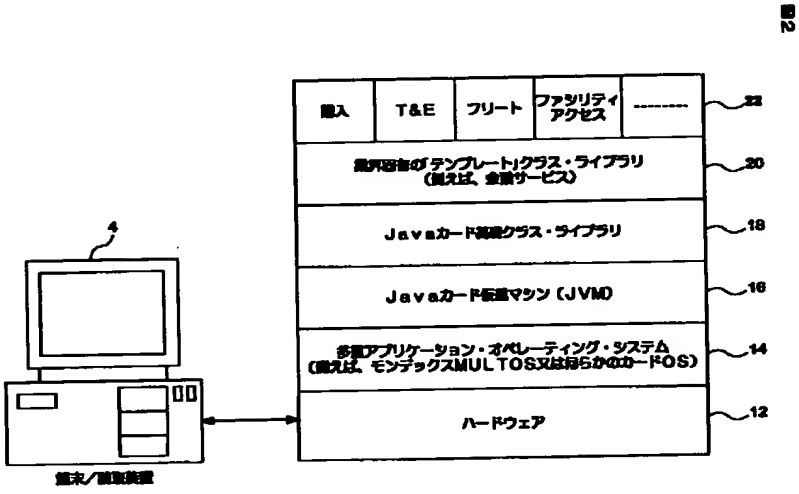
【図３】本発明の実施形態のための、図１に示す情報の流れを拡大し、アプレットを選択して確実にスマートカードへダウンロードするプロセスに関する、更なる詳細を提供する概略ダイアグラムであり、

【図４】本発明の実施形態のためのアプレットを選択して確実にスマートカードへダウンロードするプロセスに関する、更なる詳細を提供するフローチャートである。

【図1】


2
6
4
8
ネットワーク
ウォレットを使って
カードからカードへ
2
10

【図2】


購入
T&E
フリート
ファシリティ
アクセス

22
20
Javaカード実行クラス・ライブラリ
18
Javaカード仮想マシン（JVM）
16
多重アプリケーション・オペレーティング・システム
14
ハードウェア
12
4

【図3】

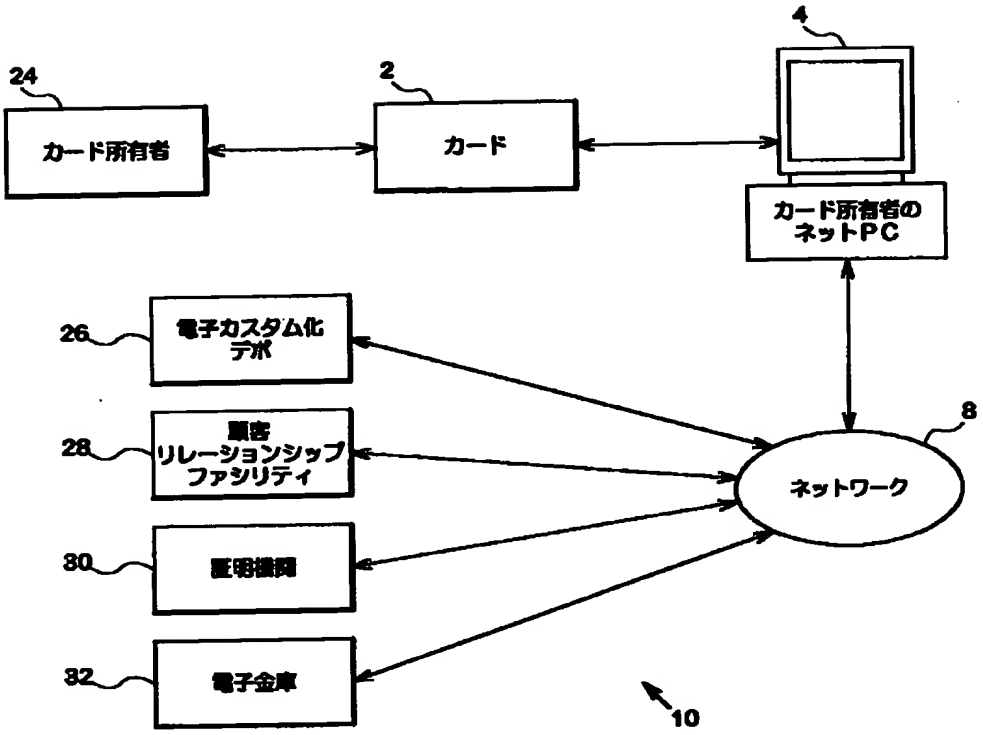
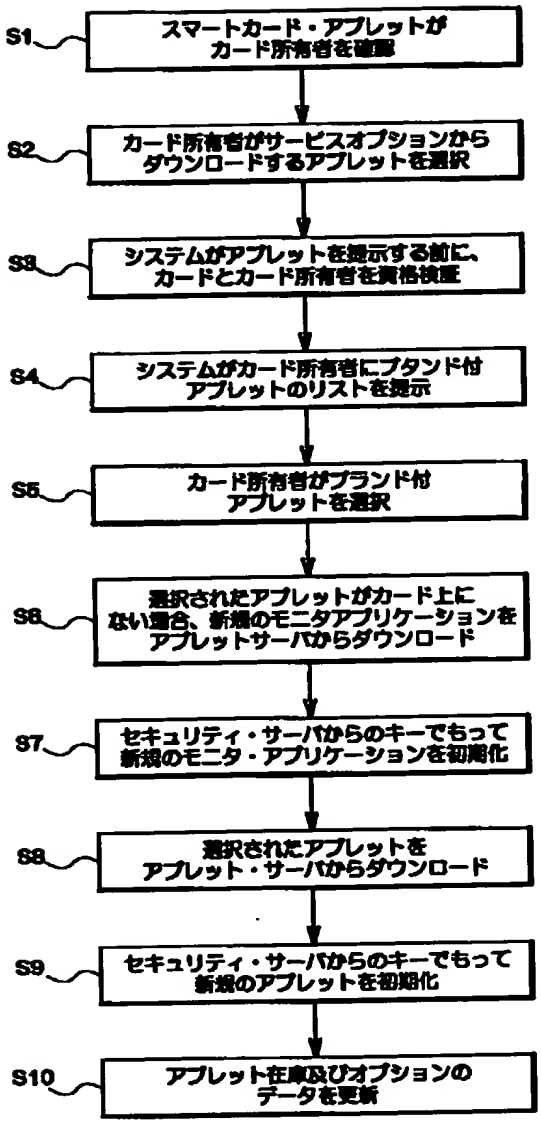


図3
4
24
2
カード所有者
カード
カード所有者の
ネットPC
26
電子カスタム化
デポ
8
28
顧客
リレーションシップ
ファシリティ
ネットワーク
30
証明機関
32
電子金庫
10

【図4】

図4



フロントページの続き

(71)出願人　598156527
12731 W. Jefferson Boulevard, Los Angeles, California 90066, U. S. A.

(72)発明者　マーク　エイ．ガズマン
アメリカ合衆国　カリフォルニア州　92586，スタディオ　シティ，シェイディグレイド　アヴェニュー　4128

(72)発明者　ニック　ボイド
アメリカ合衆国　カリフォルニア州
90066，ロス　アンジェルス，ソウテリ
ブールバード　3617

(72)発明者　ヨシフ　スムシュコヴィッチ
アメリカ合衆国　カリフォルニア州
90403，サンタ　モニカ，＃3，セカンド
ストリート　1041

(72)発明者　フレッド　ピン
アメリカ合衆国　カリフォルニア州
91406，スタディオ　シティ，ローレル
テレス　ドライヴ　12191

【外国語明細書】

METHOD AND SYSTEM FOR MANAGING APPLICATIONS FOR A MULTI-FUNCTION SMARTCARD

Cross-Reference to Related Applications

This application claims the benefit of U.S. Provisional Application No. 60/079,803 filed March 30, 1998.

Field of the Invention

The present invention relates generally to smart cards, and more particularly to a method and system for managing applications for a chip-based smartcard which has processing capability and storage capacity for more than one smartcard function.

Background

Single-function magnetic stripe cards, having a magnetic stripe on a plastic card, have been in use for many years. Such cards are based on magnetic stripe technology that can hold, for example, up to 40 characters of data on three tracks, including such information as the cardholder's name, account number, and expiration date. Existing credit, debit, and pay phone cards are magnetic stripe based.

Single-function chip cards having, for example, an 8-bit microprocessor chip, such as 8051 or 6805, embedded in the plastic card offer limited processing capability and memory storage capacity, such as 1 to 2K E^2PROM. Such cards support a single function, such as stored value, and offer better security via tamper-resistant hardware and reduced on-line transaction and infrastructure costs over magnetic stripe cards. The contents of such cards are fixed at the time of issuance.

Multi-technology hybrid cards blend more than one card technology into a single card. Technologies that are applied to such cards include magnetic stripe,

2-D bar code, optical stripe, and chip. The rationale behind such a combination is to leverage the processing power of a chip with either the backward compatibility of the magnetic stripe or the storage capacity of the 2-D bar code or optical stripe. With regard to the chip-optical combination, a combination reader is capable of reading and writing both the chip and optical stripe portions of the card.

Other cards combine contact and contactless technologies. Contactless cards are the functional equivalent of contact cards but use radio frequency technology to interact with the card reader instead of being inserted into a device. A card with contactless technology transmits transaction data and records the data that it receives when passed within either one millimeter (close coupling), 8-10 centimeters (proximity), or 0.5-1 meter (vicinity) of the reader. With contactless cards, transaction times are reduced 20 to 30 times as compared to cards requiring insertion into a device. Such combination cards offer the convenience, performance, and reliability of a contactless card, along with the security and functionality of a contact card. These cards have gained popularity as facility access and mass transit applications, such as bus, train, subway, and ferry, and have emerged as viable smartcard applications, especially when they are combined with payment methods on a single card.

While static multi-function chip cards are capable of handling multiple functions that were masked into E^2PROM at the time of card initialization, they are static because applications and functions are fixed once the card is issued.

The smartcard industry has been around since the 1970s. However, with the exception of Europe, most of the world has not gone much beyond trials and pilots. For example, financial institutions, such as banks, have introduced stored value cards, such as VISA CASH and MONDEX, to customers and merchants in pilot programs. In such pilot programs, stored value cards have been tested in densely populated areas to help reach a critical mass of acceptance in the

marketplace of consumers and merchants and to establish interoperability at merchant point of sale (POS) terminals.

While the increasing rate of smartcard usage is encouraging, it is also evident that single-function smartcards, such as stored value or pay phone cards, are a hard sell in the United States. This is mainly due to the convenience of cash and the ubiquity of credit card usage. Hence, stored value applications, at best, can be considered applications that are necessary elements of any real world smartcard programs, but are not sufficient in themselves to create a critical mass of smartcard acceptance.

Since its inception in the 1970s, a first movement in the smartcard industry began at the genesis of the technology, when a chip-based plastic card was developed to replace its magnetic stripe counterpart. Such a card offered added security and reduction in costs associated with on-line transactions and their underlying infrastructure support. A second movement can begin in the smartcard industry with the advent of a dynamic, multi-function smartcard.

The United States had little active involvement in the first movement, because of the establishment in the telecommunications infrastructure and the ubiquity of credit card usage. However, the United States can be a leader in the second movement, because of reliance by the electronic commerce industry on the smartcard to offer much needed portability, security, encryption, and authentication. Development of technologies, such as a Java card platform can allow the smartcard industry to realize the advantage of "write once, run anywhere" in which an application needs to be written only once and can then run on any card from any manufacturer.

Summary of the Invention

It is a feature and advantage of the present invention to provide a method and system for managing applications for a multi-function smartcard, which allows cardholders to carry less cash and affords cardholders nomadic access to financial and other services at any time or place and via any device.

It is a further feature and advantage of the present invention to provide a method and system for managing applications for a multi-function smartcard, which enables cardholders to organize personal information.

It is an additional feature and advantage of the present invention to provide a method and system for managing applications for a multi-function smartcard, which allows cardholders to carry fewer cards and to use the same card to conduct a suite of applications.

It is another feature and advantage of the present invention to provide a method and system for managing applications for a multi-function smartcard. which offers cardholders a means to back up their valuable information on the card.

It is a still further feature and advantage of the present invention to provide a method and system for managing applications for a multi-function smartcard. which affords cardholders the ability to store all types of information, such as emergency information or insurance information on the card.

It is still another feature and advantage of the present invention to provide a method and system for managing applications for multi-function smartcard. which can be customized by cardholders selecting applications based on personal needs and preferences.

To achieve the stated and other features, advantages and objects of the present invention, an embodiment of the invention provides a method and system for managing applications for a multi-function smartcard, such as adding new applications or applets to the smartcard for a cardholder, which includes, for

example, installing a monitor application for the new application on the smartcard microcomputer, authorizing download of the new application by the monitor application and by a master application resident on the smartcard, and downloading the new application to the smartcard microcomputer. Key hardware components of the system include for example, the smartcard embedded with a microcomputer, a terminal, a network, and a server, such as a financial institution server. Important aspects of the card application platform are the master application and the monitor application. The master application serves as an arbiter, a gatekeeper, and a message dispatcher on the smartcard, and the monitor application is a special applet supplied by an applet provider, which controls the installation of the provider's applet or applets on the smartcard.

In an embodiment of the present invention, the monitor application is installed, for example, by downloading the monitor application from a server, such as an electronic customization depot, which includes functionalities of either or both of an applet server and a monitor application server. The monitor application is downloaded, for example, at a terminal, which is any one of a number of access devices, such as an automated teller machine, a merchant terminal, a personal computer, a personal digital assistant, a TV set-top box, a land phone, a cell phone, a digital phone, a cable TV box, a satellite TV box, a contact reader, a contactless reader, or a combination contact and contactless reader. The monitor application is downloaded, for example, at the terminal from the server over a network, which is either public or proprietary. In any event, initializing the monitor application with a key provided, for example, by a server, either during initialization of the smartcard or after the smartcard has been issued, is an aspect of authorizing download of the new application. Another aspect of authorizing download of the new application is registering an application identifier for the new application with the monitor application and subsequently with the master application for dispatching of messages.

In an embodiment of the present invention, a security aspect of downloading the new application to the smartcard is verifying the identification of the cardholder, for example, by an application on the smartcard microcomputer. Such identification is done, for example, by a PIN of the cardholder or with biometric data for the cardholder. The latter is performed, for example, by a scanner at the terminal, and the biometric data, such as the cardholder's finger print, is compared with a reference template on the smartcard. Another security aspect of downloading the new application is authenticating the smartcard, for example, by the server.

In an embodiment of the present invention, the cardholder is offered a selection of service options by the system, including the option to download a new application to the cardholder's smartcard. Upon selecting the option to download a new application, the cardholder is offered a list of qualified new applications, according to pre-defined parameters, from which to select. The pre-defined parameters include, for example, whether a particular new application is supported by business based on the relationship between the cardholder and the financial institution, and whether there is sufficient space on the smartcard microcomputer to accommodate a particular new application.

In an embodiment of the present invention, the cardholder makes a selection of a new card application from the list of qualified new applications, and the new application is downloaded to the smartcard from the server, such as the electronic customization depot, which has either or both of applet server and monitor application functionalities. The new application is downloaded at the terminal, which is any one of the smartcard access devices, such as an automated teller machine, a merchant terminal, a personal computer, a personal digital assistant, a TV set-top box, a land phone, a cell phone, a digital phone, a cable TV box, a satellite TV box, a contact reader, a contactless reader, or a combination contact and contactless reader.

In an embodiment of the present invention, the new application is downloaded over the network, which is public or proprietary, and installed on the smartcard microcomputer. The new application is installed using a security mechanism of the monitor application, and the new application is supplied with an operation key. The new application is also supplied with cardholder information, as well as a new digital certificate. The new application is registered in a software registry of the smartcard microcomputer, according to an object-oriented classification of the software registry. A copy of the smartcard registry is furnished to an electronic deposit box of the financial institution, and the electronic deposit box is updated with a copy of operational data for the new application. At least one object of the new application is selectively shared with at least one object of another application on the smartcard, and the selective sharing is one or both of restricted and unrestricted sharing by the new application.

Additional objects, advantages and novel features of the invention will be set forth in part in the description which follows, and in part will become more apparent to those skilled in the art upon examination of the following or may be learned by practice of the invention.

Brief Description of the Drawing

Fig. 1 is a schematic diagram which shows an overview of examples of the key components and the flow of information between the key components of the system for an embodiment of the present invention;

Fig. 2 is a chart which shows a sample of layered hierarchy in the smartcard platform for an embodiment of the present invention;

Fig. 3 is a schematic diagram which amplifies the flow of information shown in Fig. 1 and provides further detail regarding the process of selecting and

securely downloading an applet onto the smartcard for an embodiment of the present invention; and

Fig. 4 is a flow chart which provides further detail regarding the process of selecting and securely downloading an applet onto the smartcard for an embodiment of the present invention.

Detailed Description

As smartcard technology has evolved from the single function magnetic stripe card, the cost of each card technology is proportional to the capability it delivers. For example, a rough estimate of cost for various card technologies ranges about $0.15 per card for single function magnetic stripe cards, about $2.50 for a single function chip card, about $3 per card for multi-technology hybrid cards, about $4 for a static multi-function chip card, and about $7 per card for contact-contactless combination cards. A rough estimate of the cost of a multi-function chip card for an embodiment of the present invention is in the range of about $9. Moore's law, which projects that chip processing power doubles while the cost reduces in half every 12 to 18 months, indicates that as the demand for a multi-function card rises over time, the corresponding cost will decline steadily as time passes.

In an embodiment of the present invention, a cross-industry multi-function smartcard can handle more than one application and can support the installation of new applications after the card has been issued. Application functions of a multi-function smartcard include, for example, payment vehicles, such as credit, debit, and stored value. Other functions of a multi-function smartcard include, for example, access keys for facility and network access, information manager for managing an individual's profile, demographic, and preference information, cryptographic engine for conducting encryption and authentication, and marketing tool for loyalty programs and coupons.

In an embodiment of the present invention, given the possible combinations of application functions, a multi-function smartcard serves as a bridge between the physical world and the virtual world. For example, a cardholder can use the same card to conduct purchases over the Internet and at merchant POS terminals. A smartcard infrastructure platform, such as a Java card platform, supports a multi-function card environment which is open, secure, multi-functional, dynamically downloadable, chip platform independent, and broad programmers based.

In an embodiment of the present invention, it is noted that the term multi-function and multi-application smartcards have different meanings to different groups of people. The differences are articulated as differences between a function and an application. A function is a generic concept, while an application is the actual realization of the concept in a particular implementation. For example, electronic purse or stored value is a function, while, for example, VISA CASH or MONDEX purse is an application. The correspondence between the two is many-to-many, in that many applications can be classified into a single function, as in the case of electronic purse, and many functions can be embodied in a single application. For example, Visa's VIS application consists of both credit and debit functions. Therefore, a multi-function smartcard is defined, for example, as a chip-based plastic card equipped with the necessary processing capability and storage capacity to handle more than one smartcard function, and thus more than one application, which are either installed at the time of issuance or loaded during runtime.

In an embodiment of the present invention, a broad platform strategy is applied from end-to-end, allowing simultaneous download and upgrade of software, from the card to the terminal and, ultimately, to the server. The system provides a flexible distributed architecture, whereby the intelligence or processing capability is distributed throughout the system. For example, depending on

application needs and business requirements, migration of processing capabilities from a terminal, such as an electronic wallet, to the card or to the server is permitted. With such an end-to-end perspective, system-wide concerns such as security, performance, interoperability, and standardization are reflected and addressed.

In an embodiment of the present invention, industry-specific application templates or generic applications are created that can be derived or inherited to produce specialized applications. Templates facilitate reuse, enable customization, and promote interoperability. Standards and interoperability are tightly coupled, and standards enable interoperability. Toward that end, a reinvigoration of the EMV standard adds stored value to the existing debit and credit functions. Similarly, incorporation of smartcard capability in the Secure Electronic Transaction (SET) standard solidifies a chip-electronic commerce vision as the industry moves forward.

In an embodiment of the present invention, there are, for example, three areas of primary focus in the development of a card application platform. One such area is secure dynamic application download, which includes, for example, policies and mechanisms for securely installing card applications on a smartcard after the card has been issued. Another such area is on-card application interactions, which includes, for example, mechanisms for allowing card applications to discover and safely interact with each other. An additional such area is off-card application interactions, which includes, for example, mechanisms for supporting secure interactions between on-card and off-card applications and for supporting advanced system management.

In an embodiment of the present invention, a dynamic multi-function chip card has on-card infrastructure support to facilitate post-issuance download of new applications. It is dynamic because card applications can be added or deleted after the card is issued, and an embodiment of the present invention provides an

end-to-end architecture to facilitate such an operation. Relationship cards, such as Bankcard and Citicard, have traditionally been the vehicle for extending services, for example, to customers of a financial institution, such as Citibank. A multi-function card provides a relationship card for the financial institution that integrates, for example, stored value (pay before), debit (pay now), credit (pay later), and Citicard (ATM access), with other cross-industry services as part of the financial institution's overall strategy to broaden and deepen the relationships with its customers. Further, by incorporating the credit functionality, such as Bankcard, as part of the relationship, the financial institution maintains its brand leadership while extending financial services relationship, for example, for Bankcards.

In an embodiment of the present invention, the multi-function smartcard affords nomadic access by the portability and mobility of multi-function smartcards. Such cards are an essential part, for example, of a new distribution model, in that the cards are used for access at a multiplicity of delivery vehicles, such as the Internet, GSM phone, cable, and WebTV, over all distribution channels. With such nomadicity, a multi-function smartcard enables a customer to conduct financial services anywhere, anytime, and via any device.

In an embodiment of the present invention, a multi-function smartcard supports and maximizes the global position of a financial institution, such as Citibank, in consumer and business electronic commerce, as the financial institution's core business lies in the transfer of value or movement of money and the extension of credit and related services. Lack of security and resulting proneness to fraud inherent in magnetic stripe cards costs financial institutions millions of dollars each year. The tamper resistant hardware and on-card infrastructure support of smartcards offers added security and cost savings for issuers and customers alike.

In an embodiment of the present invention, a primary benefit offered by a multi-function smartcard is convenience. Such cards provide great value to consumers, for example, by allowing consumers to carry less cash, by affording consumers nomadic access to financial and other services anywhere, anytime, and via any device, and by helping consumers to organize personal information. Another benefit which such cards offer consumers is consolidation. Consumers are attracted by the idea of combining everything in one place or in one card. Consolidation allows consumers to carry fewer cards in their wallets and to use the same card to conduct a suite of applications. Such a card is truly the ultimate thin client. As more and more information is consolidated on the card, an issue arises about the potential loss of the card. The financial institution offers a means for its customers to back up their valuable information on the card, which puts the financial institution in a unique market differentiating position and further strengthens its relationship with its customers.

In an embodiment of the present invention, a further benefit afforded customers by such a card is information storage. The concept of storing information on the card is a powerful proposition to consumers. This not only saves time, as in the case of filling forms, but can also be lifesaving, as in the case of storing important emergency information, such as allergies to medications or insurance information. A still further benefit afforded to customers by such a card is customization. With the dynamic downloadability of the multi-function card environment, consumers are able to customize the card by selecting applications based on personal needs and preferences. This puts the control of the card back to the consumer so that the card truly reflects the consumer's personality and lifestyle.

An embodiment of the present invention moves from a terminal-centric world to a customer centered, smartcard-centric world in which the smartcard is regarded as the ultimate thin client. The smartcard holds the cardholder's

identity, such as biometrics, along with other payment and access vehicles that allow the cardholder to conduct transactions anywhere, anytime, and via any device. With such portability, the smartcard can truly enable nomadic access to the various services through both the physical and the virtual worlds.

In an embodiment of the present invention, interoperability means different things at different levels of an end-to-end architecture. In essence, it means that two or more applications or participants can use each piece of the infrastructure, such as the card itself, the terminals interacting with the cards, the electronic customization depot for card applications, the acquisition and card management systems, and the settlement systems. Interoperability is a foundation necessary for operating multi-function cards and is thus a very important feature of the multi-function smartcard in the electronic commerce industry. Interoperability is a vital feature at all levels and is in place, for example, in the card infrastructure, among card applications, at the terminal-to-card interaction, and within the network infrastructure.

In an embodiment of the present invention, at the card infrastructure level, the system has a standardized virtual machine interface and the supporting class libraries, such as provided by a Java card infrastructure. At the card application level, in order for applications from different service providers, that are either within an industry or across industries, to interact with one another, the system has a set of pre-defined interaction models at the terminal or network system, as well as in the card infrastructure, such as the Java card infrastructure. At the terminal level, terminals are powerful enough such that different cards with different applications can be read on more than one terminal type. For example, an airline loyalty terminal is able to read stored value cards to speed payment, and secure access applications work in electronic ticket, gate access environments. At the network infrastructure level, a network infrastructure supports multiple

application messaging scheme and/or communication protocols, as well as application downloads.

In an embodiment of the present invention, a card platform, such as the Java card platform, serves as a standard for smartcard infrastructure. A card platform, such as the Java card platform, as the infrastructure for the smartcard is designed to achieve interoperability of applications both on the card and at the terminal. Specifically, a smartcard application designed for the Java card can run on or be added to any card supporting Java Virtual Machine (JVM) and Java class libraries. Similarly, interoperability at the terminal is achieved when the terminal has a low-level card agent or service provider that is capable of conversing with Java card applications on the other end. In such an environment, cards issued by different vendors seamlessly run on terminals from any vendors with varying capabilities.

In an embodiment of the present invention, while financial services applications have been prototyped on the Java card 1.0 platform, for example, via Schlumberger's Cyberflex cards, cross-industry applications utilize the next generation smartcard platform, such as the Java card 2.0 specification. This platform serves to demonstrate the capability of such a multi-function card environment and to demonstrate how new applications can be added to the card post-issuance. Looking beyond the card infrastructure, an architectural innovation enables development of a coherent end-to-end application. A suite of platforms, such as Java platforms, is identified that are intended for different delivery devices and systems. In descending order of scope, such Java platforms encompass, for example, Java JDK, personal Java, embedded Java, Java wallet, Java card, and picoJava.

In an embodiment of the present invention, templates are the basic definition of applications which are essential in defining a generic application such as stored value, loyalty, or telecommunications. They are the basis on which

can be built specific, branded versions of the application for a financial institution's customers. Templates are about function rather than branded identity. In a more technical sense, templates offer the foundation for building generic applications. Template facilitates reuse, thus shortening the development cycle. Specialized applications are enhanced from generic ones. Templates facilitate interoperability between applications, subject to firewalls. Therefore, it is advantageous to have a baseline stored value application that works in the same way across, for example, MASTER CARD/MONDEX, VISA, and EUROPAY.

In an embodiment of the present invention, industry-specific application templates, or generic applications are created that can be derived or inherited to produce specialized applications and achieve interoperability at the card application level. Card application development is coordinated by the use of templates. Templates facilitate reuse, enable customization, and promote interoperability. In order to facilitate the process, Smart Card Special Interest Groups, or SIGs (one per industry segment) are formed. Each SIG is responsible for individual industry template development. The task is similar to the work done by the travel industry, under the IATA Smart Card Subcommittee and IATA Resolution 791 to specify an Airline ICC.

In an embodiment of the present invention, standards and interoperability are tightly coupled, and standards enable interoperability. Toward that end, the EMV standard is re-invigorated to add stored value to the existing debit and credit functions. This enforces a unified electronic purse definition covering the functionality offered, for example, by VISA, PROTON, and other stored value products. Similarly, the SET standard incorporates smartcard capability to solidify a chip-electronic commerce vision as the industry moves forward.

In an embodiment of the present invention, other standards that facilitate interoperability are, for example, Microsoft's PC/SC and NCI's Open Card Framework (OCF). Finally, financial institutions work closely with the

telecommunications and set-top box industries to assure that the next generation GSM and the set-top box systems comprehend the needs of "nomadic" access to the various financial services, including home banking and electronic commerce. This is realized by cell phones and set-top boxes offering a two-card scenario, in that a user controlled smartcard provides secure identity in addition to customized applications, while an independent card issued by the specific industry controls the access to the underlying telecommunications or Internet services.

In an embodiment of the present invention, a smartcard has present and potential future capabilities in the electronic commerce age. However, in the age of Internet and electronic commerce, security threats continue to dominate the consciousness of the technology marketplace. In order to conduct secure exchange of purchasing orders and payment authorizations, public-key based financial transactions are of essence. For example, Secure Electronic Transaction (SET) has established itself as the leading standard in the electronic commerce world. Presently, certificates are an intrinsic part of the SET process. They are stored in the PC at the consumer end. Aside from security, lack of portability or mobility is a drawback for the approach. Hence, it is necessary to maintain separate certificates, for example, for use at home and in the office.

In an embodiment of the present invention, portability concern with a smartcard is resolved by putting the certificates on the card. Difficulties created by the present certificate size (around 1 K bytes) and the necessity for a chain of certificates to conduct an authentication process are alleviated as the capacity of the card and the industry standards evolve, such that holding certificates or some cryptograms as being proposed by EMV are as feasible as storing the cardholder's PIN. Alternatively, storing one or more private keys on the card, while leaving certificates on the PC, also provides an interim solution.

In an embodiment of the present invention, verification allows the card to uniquely verify the identity and authenticity of the cardholder. The most common

verification mechanism is the use of PIN. However, the PIN mechanism is based on the secrecy of the information. If it is lost, stolen, or if the cardholder forgets, the mechanism becomes insecure or unreliable. Biometrics oriented verification offers high accuracy and confidence in identifying the owner without the burden of PIN memorization. The reference template or templates of the cardholder's biometrics, along with one or more verification algorithms is stored on the card, such that a person's personal identification never leaves the card. As an alternative to on-card template comparison, the exchange is secured between the card and the terminal. In addition, the two devices are mutually authenticated to minimize the threat of exposing the confidential information in an unsecured environment.

In an embodiment of the present invention, the smartcard is equipped with either a high-performance microprocessor or a crypto co-processor to be capable of providing privacy, integrity, confidentiality, and non-repudiation for trusted transactions. This is accomplished through encryption (DES symmetric key or RSA public key based) and authentication (comparing digital signatures). In order to alleviate concerns about time consuming, computation intensive operations, such as the RSA public key operation, techniques such as Chinese Remainder Theorem (CRT) are applied to further accelerate the computation process. Alternatively, Elliptic Curve Cryptography (ECC) also offers comparable security with shorter key length. Ultimately, it is preferable to create private keys from within the card and use the keys to generate digital signatures using, for example, 16-bit and even 32-bit RISC processors rather than older 8-bit smartcard technology.

Information stored on the magnetic stripe or in the PC has been known to be insecure and easily counterfeited or stolen. In an embodiment of the present invention, the smartcard is regarded as the hardware token that offers tamper resistance to physical attacks. In addition, information is further protected against

unauthorized access through configurable access control measures such as PIN entry or biometrics comparison for reading or writing files on the card.

In an embodiment of the present invention, the smartcard has encryption capability to secure a message exchange between the card and the terminal (or the host) by encryption or message authentication code generation (MACing) the data. Data is downloaded to the card for information update or configuration setting. Provision is made to allow uploading of data or tokens/tickets to a remote server for short-term storage or long-term backup, for example, for a cardholder who wishes to temporarily store his/her electronic tickets to a remote server before using them. Further, in order to allow the financial institution to restore a stolen or lost card, provision is made for customers to backup the information on the card.

In an embodiment of the present invention, the smartcard has the ability to download new applications after the card is issued. This goes above and beyond the normal loading of data to and from the card and allows the cardholder to customize the card functionality to meet his/her own preference. For card issuers, such as Citibank, this also enables, for example, software upgrade, addition of new applications, and introduction of security algorithms without having to re-issue the card. This is an attractive business proposition from the perspective of total cost of ownership.

In an embodiment of the present invention, a number of categories of card applications are provided which are not mutually exclusive. In migrating from a single-function card environment to a dynamic, multi-function card world, financial institutions and consumers may aggregate applications from one or more of the categories. For example, payment applications, such as debit, credit, and stored value can co-exist with such applications as loyalty program, facility access, and network access.

In an embodiment of the present invention, classification of applications into groups formulates a strategy which establishes a framework for developing applications within individual group or industry. For example, an information manager group is regarded as a generic template or, more precisely, a base class that, for example, can be enhanced to derive specialized applications, such as profile, demographic, and preference applications. Such a framework establishment is exploited to facilitate reuse and enable customization. In establishing a coherent interface across related applications, the accessibility to the grouped services for both on-card or off-card applications, such as an electronic wallet, is also maximized. Such a design principle lays the foundation in organizing applications for additional financial institution smartcard initiatives and drives toward standardization of interfaces for individual category or class of applications.

In an embodiment of the present invention, the stored value application offers a first view of what smartcard can offer as a cash replacement in an off-line environment. The payment applications are elements in a multi-function card environment. An integrated payment card includes all three payment methods, namely, debit, credit, and stored value, for consumers. The payment card serves as a bridge between the physical and the virtual worlds in the electronic commerce age. In addition to such open currency payments, other closed payment vehicles (in a form of barter) include, for example, electronic tickets and transit tokens (as a form of payment to the system), and theme parks tokens (used in a closed entertainment environment, such as GameWorks and Disneyland). Leveraging the stronger identification and verification capabilities, electronic benefits (another form of payment) are paid through the smartcard as well.

In an embodiment of the present invention, conducting secure and trusted transactions over the physical or virtual world requires, for example, a two-tier process of verification and authentication. The cardholder's identity is verified.

and there is a mutual authentication between the card and the interacting device or server. In holding a cardholder's identity in the form of a PIN or a biometric template like finger print, the smartcard offers a means for secure access of facilities and networks by conducting or facilitating the verification process. The former requires the template matching algorithm to be resident, for example. on the card such that the verification is done locally.

In an embodiment of the present invention, once the cardholder's identity is successfully verified, the smartcard then performs mutual authentication with a terminal or a remote server to ensure a trusted transaction. Given such capabilities, the card behaves as the access keys in both the physical world for facility access and the virtual world for network access and E-commerce transactions. A generic cryptographic framework is established as the foundation for developing cryptographic applications. Such a framework allows use of such services for both on-card and off-card applications to maximize reuse and shorten the time-to-market.

In an embodiment of the present invention, the smartcard enhances a trusted relationship between, for example, a bank and its customers, based on the secure storage of both value and information of the cardholder. Several types of information pertaining to a cardholder can be stored on the card. For example. personal identification , such as name, blood type, date and place of birth. mother's maiden name, address, and phone number can be stored. Profile and demographic information, such as marriage status, number of children and their ages, income level, and hobbies can also be stored. Further, preference information, such as language, frequent calling numbers, airplane seat assignment, and computer configuration can be stored on the card. Additionally, privilege and entitlement information, such as administrative status for computer and network access can be stored on the card.

In an embodiment of the present invention, the smartcard plays the role of an information manager on behalf of the cardholder that safeguards and manages the cardholder's personal information. This is important as consumer privacy is a leading concern in the smartcard and electronic commerce industries. Different kinds of information require different levels of security measures to authorize an access. Much of the trusted relationship between a financial institution, such as a bank, and its customers hinges on how well the financial institution manages its customers' personal information. A flexible yet secure information access mechanism is provided, such that applications like filling forms at a doctor's office can be automated without the concern of invasion of privacy.

In an embodiment of the present invention, the smartcard provides a marketing tool for both merchants and financial institutions by storing loyalty points or coupons for individual retailers. On-card loyalty applications provide cardholders flexible shopping benefits, including instant loyalty points reward and redemption, for both physical and Internet transactions. In addition, churches and schools can, for example, issue scrips to benefit their causes from the sales.

In an embodiment of the present invention, by allowing download of new applications after the card is issued, the smartcard offers a unique delivery channel in distributing customized services. The cardholder can determine the applications on the card and make adjustments as his/her lifestyle evolves. For example, the cardholder can delete rarely used applications and add new ones. The personalization capability is further amplified in conjunction with a multiplicity of delivery channels, such as cell phones, set top boxes, and network computers. Consumers are afforded added convenience and flexibility in conducting financial transactions and invoking services delivered through the smartcard.

Referring now in detail to an embodiment of the present invention, which is illustrated in the accompanying drawings, Fig. 1 shows an overview of the key

components from a system-wide perspective of the architecture for an embodiment of the present invention. Referring to Fig. 1, the end-to-end architecture takes into account the issues and concerns from the card 2 to the terminal 4, to the front-end system 6, to the network 8, and, ultimately, to the back-end server 10. Such an end-to-end perspective is an important aspect of the system and enables reflecting and addressing system-wide concerns, such as security, performance, interoperability, and standardization. In this multi-function world, it is imperative to have such an understanding in order to gauge the needed performance and security for the card. This also enables addressing the interoperability and standardization concerns between the card 2 and the terminal 4, as well as between the terminal 4 and the back-end server 10. For example, the system architecture is designed such that security broken on one end can be remedied or minimized from the other.

Referring further to Fig. 1, five major components of the end-to-end architecture include, for example, the smartcard 2, the terminal 4. the front-end 6. the network 8, and the back-end servers 10. The card issuer has full control of the security measures both on the card 2 and at the back-end servers 10. The in-between terminals 4 and 6 and the networks 8 are regarded as insecure and are treated with special attention. On the other hand, intelligence or processing capability is distributed across the system. Depending on the application needs. intelligence is propagated from the card 2 to the terminal 4, and to the servers 10. or vice versa.

In an embodiment of the present invention, the smartcard 2, acting as the ultimate thin client, is the relationship card that is leveraged to further the trusted relationship between a financial institution , such as a bank, and its customers. In order to accomplish that, the card infrastructure supports the required multi-functionality and downloadability. An example of such a platform is Java card. which encompasses the virtual machine and the supporting class libraries. Fig. 2

is a chart which shows a sample of layered hierarchy in the card platform for an embodiment of the present invention. A card platform, such as the Java card platform, offers a layered hierarchy in its architecture. For example, a Java card virtual machine (JVM) 16 sits atop the card operating system 14 that is either proprietary or open, as in the case of Mondex's MULTOS.

In an embodiment of the present invention, the term applet means a smartcard application that is compact in size and downloadable over a public network. Referring to Fig. 2, a card architecture such as JVM 16 offers added security during runtime by providing bytecode verification to prevent unauthorized applets from being executed on the card. Bytecode is machine independent and is interpreted by the JVM 16. Sitting above the JVM layer 16 are the foundation class libraries 18, which offer the interface for building Java card applications. Such a framework based approach facilitates reuse and enables faster time-to-market for the application development. In order to further extend that vision, industry-specific and application-specific templates 20 are created, which are foundation class libraries that can be derived or inherited to produce specialized applications. Hence, interoperability is achieved at the card application level. Finally, at the top of the hierarchy is a suite of cross-industry applications 22 that co-exist harmoniously on the card 2.

In an embodiment of the present invention, a spectrum of terminals and access devices 4 have smartcard interfaces. These include ATMs, POS terminals, PCs with smartcard readers (either standalone or part of keyboards), personal digital assistants (PDAs), set-top boxes, cell phones, cable/satellite TV boxes, and various contact/contactless reader devices. The design provides a coherent architecture between the card 2 and the terminal 4, such that both card and terminal applications can be upgraded simultaneously to allow seamless migration. An electronic wallet residing, for example, on a PC or distributed over a network offers a vehicle for delivering payment services and information

management over the Internet. The smartcard 2 is a natural extension of the wallet to physically contain some of the wallet functionalities. The smartcard 2 evolves as the physical embodiment of the wallet. Thus, a certain portion of the wallet functionalities are moved to the card 2, while others either stay on the terminal 4 or browser or move to the server. Distribution of intelligence across the network is realized in such a migratory fashion.

In an embodiment of the present invention, from an architectural perspective, the data of a wallet physically resides, for example, on the card 2 or in a remote server. The storage location is arranged based on the nature of the information and the constraint of capacity on the card 2. Regardless of the physical location, the information is accessible to the user transparently. In situations where the user wishes to have a conscious understanding of the actual data location so as to make a proper decision during transactions, the smartcard architecture facilitates such a decision-making process. Storing or backing up critical information on the server is a powerful mechanism to safeguard a cardholder's valuable information.

In an embodiment of the present invention, in the event that the card 2 is lost or stolen, a financial institution can confidently issue a new card with the original card information (not stored value) restored from the financial institution's servers. With this recoverability, the customers of the financial institution have a peace of mind, knowing that a trusted financial institution is securing the information on their behalf. This, in turn, provides market differentiation for a financial institution, such as bank, as losing a card has become one of the top consumer concerns. In order to enable biometrics-based verification, a biometric scanning device, such as a fingerprint or hand geometry scanner, is installed at the terminal 4. The captured biometric data is compared with a reference template on the card 4 to verify the authenticity of the cardholder.

In an embodiment of the present invention, the front-end systems 6 serve as the front end to terminals 4. Their principal responsibility is to offer the necessary translation of message protocols between the terminal 4 and back-end servers 10. They often play the role of a middleware or gateway in a networking environment, such that smartcard-ready terminals 4 are transparent to back-end legacy systems 10. Networks 8 offer the plumbing in a distributed environment. Both public (open) and private (proprietary) networks are used in the system. The former include, for example, Internet, PLUS, Cirrus, and Star., whereas the latter includes, for example, Citishare.

In an embodiment of the present invention, in the financial services environment, back-end servers 10 deal with clearing and settlement functions. Several back-end services support operations in a dynamic, multi-function environment, such as Certificate Authority (CA), Electronic Customization Depot (ECD), Electronic Deposit Box (EDB), and Electronic Vault (EV). A financial institution can provide one or more of such services in order to provide market differentiation and to further the relationships with its customers. The particular services are devised logically according to their functions. More than one service can reside physically on the same server 10, depending on business needs and design decisions.

In an embodiment of the present invention, Certificate Authority (CA) is a trusted third party. It is responsible for issuing certificates to customers, merchants, and those who want to conduct public-key based transactions over the Internet. Secure Electronic Transaction (SET) operations are certificate based. Thus, the CA inherently becomes an integral part of any secure transaction process. A financial institution can be a CA in order to maximize interactions with its customers.

In an embodiment of the present invention, an electronic customization depot behaves as an applet server and a monitor application server to offer a

customer the options to customize the customer's card 2 by adding or deleting applets. As an applet server, it is the source for applet download and for card restoration. Each monitor application is responsible for establishing secure download of applets to the customer's smartcard 2. Load keys, for example, are stored in the monitor application to facilitate the operation. Counterparts of a safety deposit box and vault in the physical world are provided in a virtual world electronic deposit box and electronic vault. Like a safety deposit box, whose purpose is to store customer's valuables in a trusted and secure environment, the electronic deposit box offers similar services to a financial institution's customers.

In an embodiment of the present invention, the financial institution stores or backs up valuable information on the smartcard 2 for a customer upon request. Collectively, electronic deposit boxes are aggregated within an electronic vault. In addition to holding customers' valuable information, including electronic tokens and tickets, an individual electronic deposit box also maintains a software inventory of each customer's card 2. With such an inventory, the financial institution is able to restore the card applications, for example, from the electronic customization depot, for a customer when the card is lost or stolen.

In an embodiment of the present invention, facilities are provided to support applications, such as secure dynamic application downloads, which are the policies and mechanisms needed to securely install card applications on the smartcard 2 after the card has been issued. Other such facilities include on-card application interactions, which are mechanisms for allowing card applications to discover and safely interact with each other. Additional such facilities include off-card application interactions, such as mechanisms for supporting secure interactions between on-card and off-card applications and advanced system management. On-card applications are frequently referred to as applets. Of necessity, applications installed on the smartcard 2 tend to be very small when

compared with desktop, terminal, or mainframe applications and hence are called applets.

In an embodiment of the present invention, the smartcard application platform meets two overall security goals, namely, to ensure the security and integrity of the card's system components and to provide applets with scaleable mechanisms to ensure their own security and integrity. The overall security policy for the card 2 is that only authorized entities may have access to card resources; and this access is limited to the activities for which access has been granted. In order to insure that security goals of the financial institution are met. the card application platform includes several important elements, two of which are a master application and the monitor application. As a special system applet. the master application represents the card issuer. It provides global card services. including, for example, installing applets on the card 2, personalizing and reading global data, managing the card life cycle state, supporting external audits when the card is blocked, and maintaining a map of the monitor applications associated with each applet.

In an embodiment of the present invention, the system includes applets developed by other applet providers, as well as a financial institution's own applets. Thus, the card application platform supports the secure and confidential installation of applets from multiple providers. In order to support secure installation of applets, the financial institution uses monitor applications. A monitor application is a special applet supplied by an applet provider. Each monitor application controls the installation of a provider's applet or applets. There can be multiple monitor applications on a card. Each monitor application represents a unique cryptographic relationship for a single applet provider. Using its unique combination of cryptographic mechanisms and keys, each monitor application manages the signature checking and decryption of applets loaded onto the card 2. Therefore , the installation and initialization of a monitor application

on the card 2 is an essential step to support the secure download of a provider's applets.

Another important aspect of an embodiment of the present invention is the installation of the master application on the card 2, which functions in conjunction with the monitor application.. The master application serves, for example, as an arbiter, a gatekeeper, and a message dispatcher on the smartcard 2. Direct application-to-application interactions on the card are not permitted. Instead, all interactions must go through the master application, serving as the arbiter, gatekeeper and message dispatcher on the card 2. The master application serves as an arbiter during inter-application communications. Any request initiated by one application is sent to the master application before it is routed to its destination application, for example, for preliminary checking to prevent bogus requests. Such a request can be, for example, a file access or a service rendition. In either case, it is up to the destination or receiving application to decide whether to honor the request.

The master application serves as a gatekeeper, for example, during dynamic application downloading to prevent unauthorized applications from being downloaded onto the card 2. In such capacity, the master application, working in conjunction with the individual monitor applications, performs necessary authentication and validation functions to ensure that the downloaded application originates from a legitimate source and that the content has not been altered.

The master application serves as a message dispatcher, for example, during terminal-to-card interactions. The message dispatching process is a simple, yet robust, message routing mechanism that ensures timely delivery of messages, while incurring little overhead. Each incoming message is routed sequentially to each application resident on the card 2, and each such application determines whether it is the intended recipient of the message. If so, the

particular application processes the message and returns a "success" response. Otherwise, the application returns an "error" message, and the master application continues to forward the message to other applications on the card 2, until a "success" response is returned. Thereafter, subsequent messages are forwarded to the last successful application, until the particular application returns an "error" message, and the cycle is repeated.

Another important aspect of an embodiment of the present invention is installation of a consolidated identification application (ID application) on the card 2. The ID application serves as a single placeholder for all personal profile related information to avoid duplication of data. When an application requires identification related information, the application submits its own identification and a clearance level, and the ID application determines the privilege. if any, to be given to the requesting application for data access. For example, a health care application can access the cardholder's blood type information, while a loyalty program cannot.

In an embodiment of the present invention, the installation and initialization of monitor applications can occur during card initialization. However, for maximum flexibility, the financial institution supports downloading and installing new monitor applications after the card 2 has been issued. To support this feature, a root monitor application is installed during card initialization and personalization. Subsequently, each downloaded monitor application allows the financial institution to download and install specific applets. Before the actual download and installation of an applet takes place, the appropriate monitor application authorizes the download of the applet. Therefore, before an applet is downloaded, an application identifier (AID) that identifies the applet must be registered with the appropriate monitor application, so that it can authorize the downloading of the identified applet.

Fig. 3 is a schematic diagram which amplifies the flow of information shown in Fig. 1 and provides further detail regarding the process of selecting and securely downloading an applet onto smartcard 2 for an embodiment of the present invention. Fig. 4 is a flow chart which provides further detail regarding the process of selecting and securely downloading an applet onto the smartcard 2 for an embodiment of the present invention. At S1, the smartcard 2 contains an applet that verifies the identity of the cardholder 24 with a PIN or a biometric. such as a fingerprint. At S2, from a selection of service options offered by the system, the cardholder 24 selects the option to download a new applet. The card 2 and the cardholder 24 must both be qualified before the system offers any applets for download. At S3, the system offers those applets supported by the business based on one or more relationships with the cardholder 24 and those applets that will fit in the space available on the card 2.

In an embodiment of the present invention, it is noted that space qualifications imposed on applets must account for the total space needed for each applet, including any other applets on which each applet depends. Thus, applets may be grouped into clusters. So, if one applet depends on another applet that has not yet been installed on the card 2, the card has enough space to accommodate all applets that form such a dependency cluster. At S4, the system presents a list of qualified applets to the cardholder 24, including, for example, brands that help identify the providers of the applets. There are several kinds of disclosures to allow the cardholder 24 to make informed decisions during applet selection. Some representative examples include the total size of each applet, the space available on the card 2, and any other limitations inherent in the card infrastructure. For example, once an applet has been installed, it cannot be removed, nor can the allocated space be recovered.

In an embodiment of the present invention, at S5, the cardholder 24 selects an applet from the offered applet list. At S6, if a monitor application for the

selected applet does not exist on the card 2, a new one is downloaded from the applet server in the electronic customization depot. At S7, if a new monitor application was added to the card, the new monitor application is initialized with any necessary key or keys, which are obtained from the security server in the electronic customization depot. At S8, the selected applet is downloaded from the applet server in the electronic customization depot 26 and installed, using the security mechanism provided by the monitor application and, for example, the gatekeeper functionality of the monitor application. At S9, the security server in the electronic customization depot 26 supplies the new applet with any key or keys necessary for its operation.

In an embodiment of the present invention, if the applet requires any customer information, it is obtained from the customer relationship facility 28. If the applet requires a digital certificate, it is obtained from the appropriate certificate authority 30. At S10, if the cardholder relationship supports it, the new applet is registered in the card software inventory. A copy of the card software inventory is maintained in the cardholder's electronic deposit box in the bank's electronic vault 32. In addition, the cardholder's electronic deposit box is updated with a copy of the applet's operational data, if any, but not any keys or certificates, which are reissued in the event of a lost card.

In an embodiment of the present invention, in order to create a secure and trusted environment, applets are isolated from each other. An applet firewall prevents one applet from accessing the contents and behavior of objects owned by other applets. However, some applets are allowed to communicate with each other in trusted ways. A smartcard, such as the Java card, provides two basic mechanisms for explicitly sharing objects between applets. One such mechanism is restricted sharing, and the other is unrestricted sharing. Restricted sharing allows an applet to grant specific other applets access to a shared object. Unrestricted sharing allows an applet to grant all other applets access to a shared

object. In combination, these two basic mechanisms are used to implement selective object sharing. Some applets share selected information and services. For example, a payment applet interacts with a loyalty applet to add loyalty points as part of a payment transaction. However, the loyalty applet provider can restrict these interactions to applets from certain providers or certain kinds of payment applets. To support this kind of selective interoperability, some of the applets have a mechanism for shared object registration.

In an embodiment of the present invention, applets can be downloaded and installed on the card 2 after the card has been issued. Therefore, an applet that already exists on the card 2 does not have any knowledge of a newly installed applet until the new applet registers itself with the pre-existing applet. Once the new applet identifies itself to the pre-existing applet, the pre-existing applet can grant the new applet access to its shared object or objects. Thus, the pre-existing applet or sharing applet supports registration of other applets for its shared object or objects.

In an embodiment of the present invention, in order to implement shared object registration, the sharing applet grants unrestricted access to a resource guardian. The resource guardian controls and grants restricted access to some guarded resource or resources, referred to as the sharing applet's shared object or objects. Some of the applets can also contain reusable foundation class libraries or groups of Java classes that are generic enough to be used by several kinds of applets. In order to retain control over the usage of some objects and thereby maintain trust, some of these libraries include shared object factories. A shared object factory creates a new instance of a library class on request for a specific client applet, and registers the new instance for access by the client applet.

In an embodiment of the present invention, some applets share information and services. However, giving the cardholder 24 the ability to select and dynamically download applets implies that the applets cannot be installed on the

card 2 in a predetermined order. For example, a loyalty applet can be designed to support interactions with several kinds of payment mechanisms. When a new payment mechanism is installed on the card 2, it will likely want to discover whether any compatible loyalty applets are already on the card. Therefore, in order to allow dynamically loaded applets to discover during installation what other applets exist on the card 2, the card application platform includes an application registry.

In an embodiment of the present invention, the application registry provides a shared object registration mechanism that supports linkage between applications based on their identification and based on their functionality or object-oriented classification. Thus, newly installed applets are able to discover whether another applet exists on the card 2 using an AID, and are also be able to discover whether any other applet exists on the card that implements a specific functional interface or that was derived from a specific base class.

In an embodiment of the present invention, allowing applets to discover and link with each other based on their functionality gives them a much more flexible alternative to identification alone. It allows them to achieve a level of multi-functional integration beyond the simple deployment of multiple functions on the smartcard 2. It also allows terminals to dynamically and intelligently adapt their interactions with the card 2 based on the functionality supported by the applications that actually exist on the card. In addition to facilities that support on-card interactions, card applications also have services to facilitate interactions with off-card applications, whether they reside on the card terminal 4 or on back-end systems 10.

In an embodiment of the present invention, security mechanisms related to dynamic application download are asymmetric in that they are applied in only one direction. A downloaded applet is decrypted and its integrity and authenticity are verified before it is installed on the card 2. However, the applets themselves have

symmetric mechanisms for security. They have support, for example, for data encryption and decryption, digital signature generation and verification, and message authentication code (MAC) generation and verification. The card application platform includes a facility, such as cryptographic foundation classes, that supports packaging these diverse security mechanisms together for coherent, consistent and symmetric use, including services for key generation and key management.

In an embodiment of the present invention, as the cardholder 24 puts more and more kinds of information on the card 2, the value of the card to the cardholder naturally increases. Thus, the loss of the card 2 may represent a substantial loss for the cardholder 24. To reduce the significance of this loss, the system provides a mechanism for recovering the information contained on the card 2 in order to re-issue the card in the event of its loss. The financial institution provides a secure off-card information storage facility or electronic vault 32 that contains an electronic deposit box for each cardholder 24. Each electronic deposit box contains a copy of the contents of each card that the cardholder 24 registers with the bank, including a software inventory of the applets installed on the card 2, as well as a copy of the information managed by each of the installed applets.

In an embodiment of the present invention, applets of providers other than the financial institution can be installed on the card 2. The providers of such other applets have a legitimate interest in protecting their security keys and the data managed by their applets. In order to support applet data recovery, the applets on the card 2 and the electronic vault 32 cooperate by using a secure protocol for data exchange. In order to support applet provider secrecy, each applet uses encryption to prevent the copied data in the vault 32 from being examined. These electronic security mechanisms together mimic the physical security mechanisms used to store valuables in a safe deposit box. For example,

it requires two keys to access the valuables stored in the deposit box, one of which belongs to the customer and one of which belongs to the bank. Thus, using symmetric mechanisms, each applet is able to produce a blinded copy of its information during backup, and consume a blinded copy during restoration. The electronic vault 32 stores the blinded copy of the information for each applet.

In an embodiment of the present invention, the smartcard 2 is not limited to playing the role of a service provider in a client-server architecture, in which interactions between the card 2 and the terminal 4 are initiated by the terminal, with the card as a responsive device, but the system provides a more flexible architectural solution that includes the smartcard. On-card objects are allowed, for example, to initiate interactions with remote, off-card objects in the context of a distributed computing environment, which is supported by a card platform, such as Java card, with inclusion of, for example, the Java facility for remote method invocation (RMI).

In an embodiment of the present invention, in the context of distributed objects, mechanisms are provided by the system to support transparent object distribution. Thus, on-card objects are able to interact with off-card objects and vice-versa without explicit knowledge of their location. Such transparency simplifies the system design, allowing greater flexibility in locating objects, and supports the deployment of migratory objects that can move from one place, such as the electronic vault 32, to another, such as the card 2. For example, an electronic ticket can be bought and stored in the electronic vault 32 until, when it is needed for use, it can be moved onto the smartcard 2 to allow off-line redemption.

In an embodiment of the present invention, replacement of deployed applets is supported by a card platform, such as Java card. Application identifiers (AIDs) are assigned and administered. An applet AID can be reused without change when deploying a new applet version. Alternatively, but less desirable, is

a naming scheme for AIDs that includes a version identifier to guarantee uniqueness. A mechanism replaces the objects that have been created for an applet, for example, when some of the applet classes have changed their shapes. On-card mutation may be difficult or not possible given the card constraints. This consideration reinforces the value of the electronic vault 32 as a backup facility.

In an embodiment of the present invention, the old version of an applet may be removed entirely, including all its objects, and replaced with the new version, and the applet objects restored from backup copies that have been mutated in the electronic vault 32. A cleanroom software engineering approach for applet development applies rigorous process controls to the software development process, producing very high quality software, such as six sigma quality. The resource constraints of smartcards require that applets must be kept relatively small and simple. Thus, the rigorous process requirements of the cleanroom approach are not as burdensome as it is on large software projects.

Various preferred embodiments of the invention have been described in fulfillment of the various objects of the invention It should be recognized that these embodiments are merely illustrative of the principles of the present invention. Numerous modifications and adaptations thereof will be readily apparent to those skilled in the art without departing from the spirit and scope of the present invention. Accordingly, the invention is only limited by the following claims.

What is claimed is:

1. A method of managing addition of at least one new application to a multi-function smartcard for a cardholder, comprising:

installing a monitor application for the new application on a microcomputer of the smartcard;

authorizing download of the new application by the monitor application and by a master application resident on the smartcard; and

downloading the new application to the smartcard microcomputer.

2. The method of claim 1, wherein installing the monitor application further comprises downloading the monitor application from a server.

3. The method of claim 2, wherein the server further comprises an electronic customization depot.

4. The method of claim 3, wherein the electronic customization depot further comprises functionalities of at least one of an applet server and a monitor application server.

5. The method of claim 1, wherein installing the monitor application further comprises downloading the monitor application at a terminal.

6. The method of claim 5, wherein the terminal further comprises a smartcard access device selected from a group consisting of an automated teller machine, a merchant terminal, a personal computer, a personal digital assistant, a TV set-top box, land phone, a cell phone, a digital phone, a cable TV box, a satellite TV box, a contact reader, a contactless reader, and a combination contact and contactless reader.

7. The method of claim 6, wherein downloading the new application further comprises downloading an application consisting of at least a portion of a plurality of functionalities for an electronic wallet from a server connected to the terminal, while allowing other portions of the functionalities for the electronic wallet to remain on at least one of the terminal and the server in a migratory fashion.

8. The method of claim 1, wherein installing the monitor application further comprises downloading the monitor application over a network.

9. The method of claim 8, wherein the network further comprises at least one of a public network and a proprietary network.

10. The method of claim 1, wherein authorizing the download further comprises initializing the monitor application.

11. The method of claim 10, wherein initializing the monitor application further comprises initializing the monitor application with a key provided by a server.

12. The method of claim 1, wherein authorizing the download further comprises registering an application identifier for the new application with the monitor application.

13. The method of claim 1, wherein downloading the new application further comprises verifying identification of the cardholder.

14. The method of claim 13, wherein verifying the identification further comprises verifying the identification by an application on the smartcard microcomputer.

15. The method of claim 14, wherein verifying the identification further comprises verifying the identification with a PIN of the cardholder.

16. The method of claim 14, wherein verifying the identification further comprises verifying the identification with biometric data of the cardholder.

17. The method of claim 16, wherein verifying with the identification further comprises verifying the biometric data with a scanner at a terminal.

18. The method of claim 17, wherein verifying the biometric data further comprises comparing the biometric data with a reference template on the smartcard microcomputer.

19. The method of claim 18, wherein the biometric data further comprises fingerprint data for the cardholder.

20. The method of claim 1, wherein downloading the new application further comprises authenticating the smartcard.

21. The method of claim 20, wherein authenticating the smartcard further comprises authenticating the smartcard by a server.

22. The method of claim 1, wherein downloading the new application further comprises offering a selection of service options to the cardholder.

23. The method of claim 22, wherein downloading the new application further comprises selecting a service option to download a new application by the cardholder.

24. The method of claim 1, wherein downloading the new application further comprises offering a list of qualified new applications to the cardholder.

25. The method of claim 24, wherein the list of qualified new applications further comprises a plurality of new applications according to pre-defined parameters.

26. The method of claim 25, wherein the pre-defined parameters comprise at least one of a new application supported by business based on a relationship with the cardholder and a new application that fits in space available on the smartcard microcomputer.

27. The method of claim 26, wherein the pre-defined parameters further comprises the new application which, together with any other applications on which the application depends, fits as a dependency cluster in space available on the smartcard microcomputer.

28. The method of claim 24, wherein downloading the new application further comprises selecting the new application from the list of applications by the cardholder.

29. The method of claim 1, wherein downloading the new application further comprises downloading the new application from a server.

30. The method of claim 29, wherein the server further comprises an electronic customization depot.

31. The method of claim 30, wherein the electronic customization depot further comprises functionalities of at least one of an applet server and a monitor application server.

32. The method of claim 1, wherein downloading the new application further comprises downloading the new application at a terminal.

33. The method of claim 32, wherein the terminal further comprises a smartcard access device selected from a group consisting of an automated teller machine, a merchant terminal, a personal computer, a personal digital assistant, a TV set-top box, a land phone, a cell phone, a digital phone, a cable TV box, a satellite TV box, a contact reader, a contactless reader, and a combination contact and contactless reader.

34. The method of claim 1, wherein downloading the new application further comprises downloading the new application over a network.

35. The method of claim 34, wherein the network further comprises at least one of a public network and a proprietary network.

36. The method of claim 1, wherein downloading the new application further comprises installing the new application on the smartcard microcomputer.

37. The method of claim 36, wherein installing the new application further comprises installing the new application using a security mechanism of the monitor application.

38. The method of claim 36, wherein installing the new application further comprises supplying the new application with an operation key.

39. The method of claim 36, wherein installing the new application further comprises supplying the new application with cardholder information.

40. The method of claim 36, wherein installing the new application further comprises supplying the new application with digital certificate.

41. The method of claim 36, wherein installing the new application further comprises registering the new application in a software registry of the smartcard.

42. The method of claim 41, wherein registering the new application further comprises registering the new application according to an object-oriented classification of the software registry.

43. The method of claim 41, wherein registering the new application further comprises furnishing a copy of the smartcard software registry to an electronic deposit box.

44. The method of claim 43, wherein furnishing a copy further comprises updating the electronic deposit box with a copy of operational data for the new application.

45. The method of claim 36, wherein installing the new application further comprises selectively sharing at least one object of the new application with at least one object of another application on the smartcard.

46. The method of claim 45, wherein selectively sharing further comprises at least one of restricted sharing of the object by the new application and unrestricted sharing by the new application.

47. A system for securely adding at least one new application to a multi-function smartcard for a cardholder, comprising:

means for installing a monitor application for the new application on a microcomputer of the smartcard;

means for associated with the installing means for authorizing download of the new application by the monitor application and by a master application resident on the smartcard; and

means associated with the authorizing means for downloading the new application to the smartcard microcomputer.

48. The system of claim 47, wherein the installing means further comprises means for downloading the monitor application from a server.

49. The system of claim 48, wherein the server further comprises an electronic customization depot.

50. The system of claim 49, wherein the electronic customization depot further comprises functionalities of at least one of an applet server and a monitor application server.

51. The system of claim 48, the means for downloading the monitor application further comprises a terminal communicating with the server over a network.

52. The system of claim 47, wherein the means for downloading the new application further comprises a server.

53. The system of claim 52, wherein the server further comprises a an electronic customization depot.

54. The system of claim 53, wherein the electronic customization depot further comprises functionalities of at least one of an applet server and a monitor application server.

55. The system of claim 52, wherein the means for downloading the new application further comprises a terminal communicating with the server over a network.

【図1】

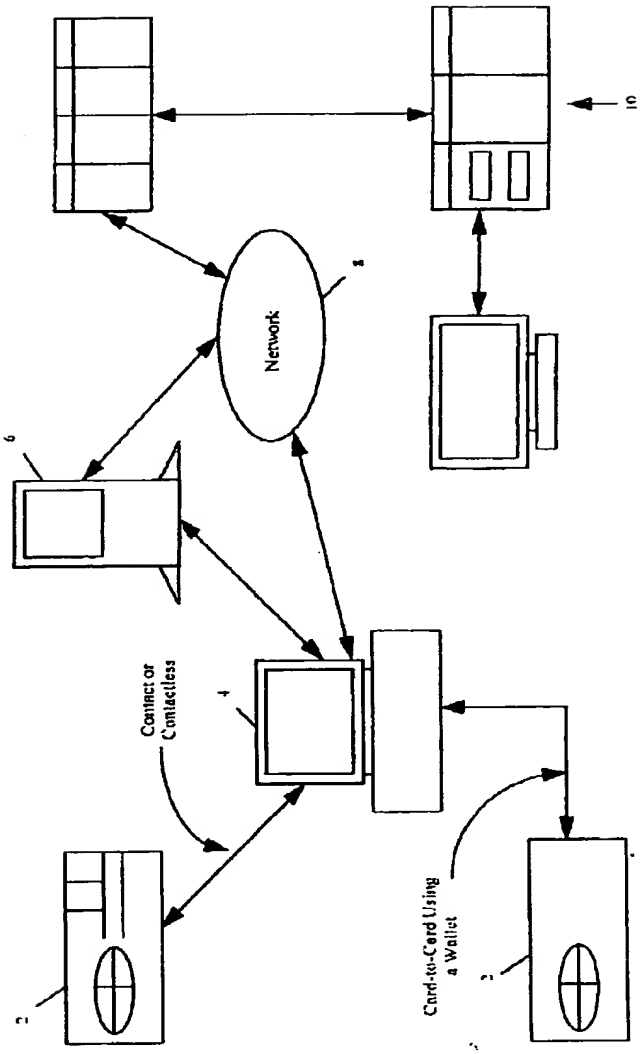


FIG. 1

【図2】

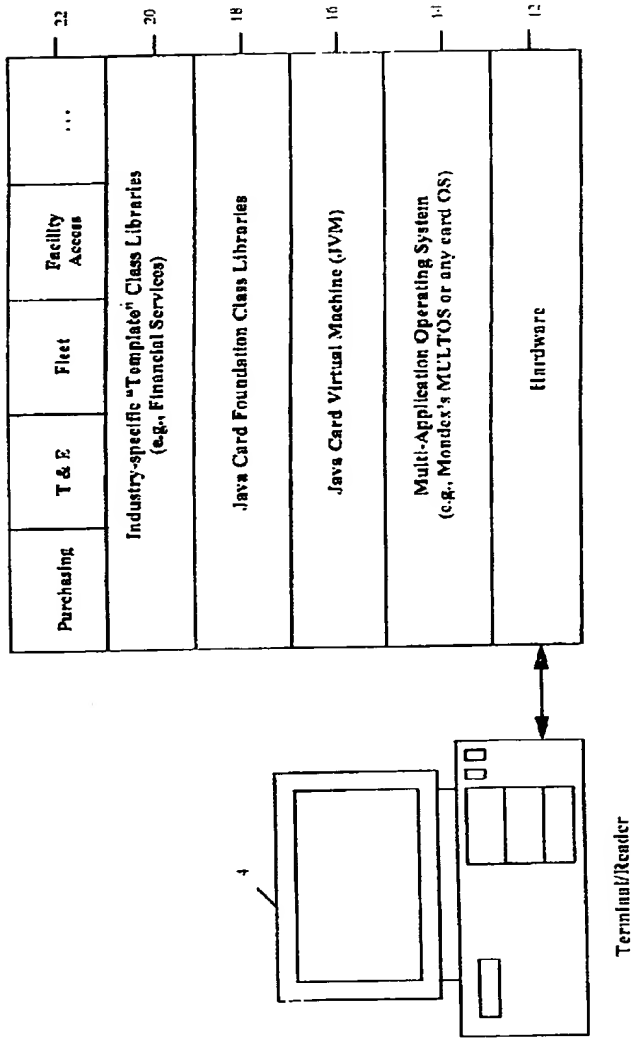

22
20
18
16
14
12
...
Facility Access
Fleet
T & E
Purchasing
Industry-specific "Template" Class Libraries (e.g., Financial Services)
Java Card Foundation Class Libraries
Java Card Virtual Machine (JVM)
Multi-Application Operating System (e.g., Mondex's MULTOS or any card OS)
Hardware
4
Terminal/Reader

FIG. 2

【図３】

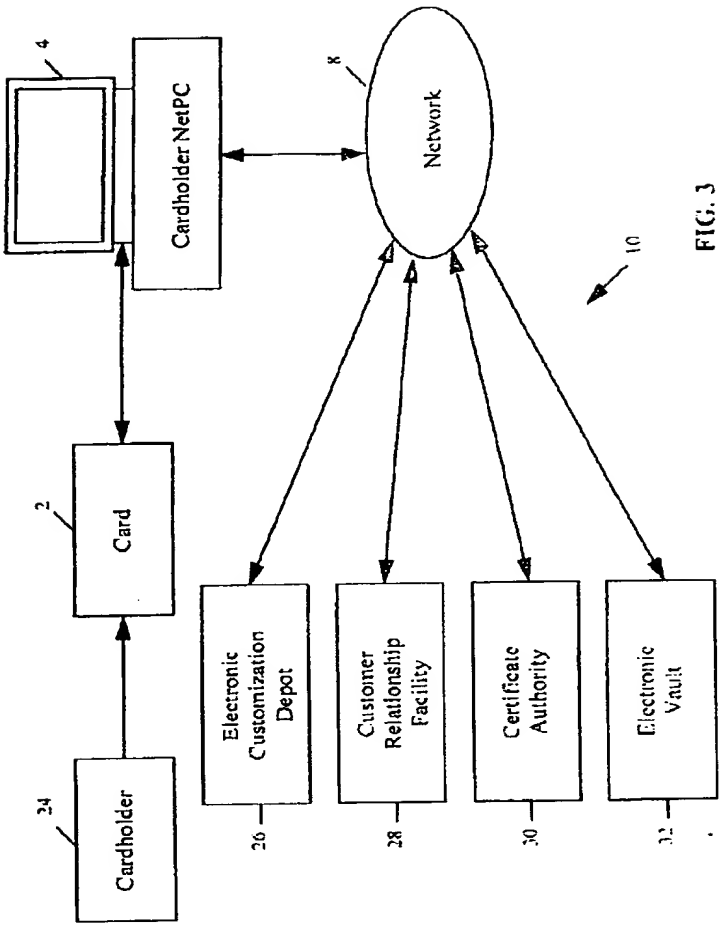

4
Cardholder NetPC
8
Network
10
2
Card
34
Cardholder
26
Electronic Customization Depot
28
Customer Relationship Facility
30
Certificate Authority
32
Electronic Vault

FIG. 3

【図4】

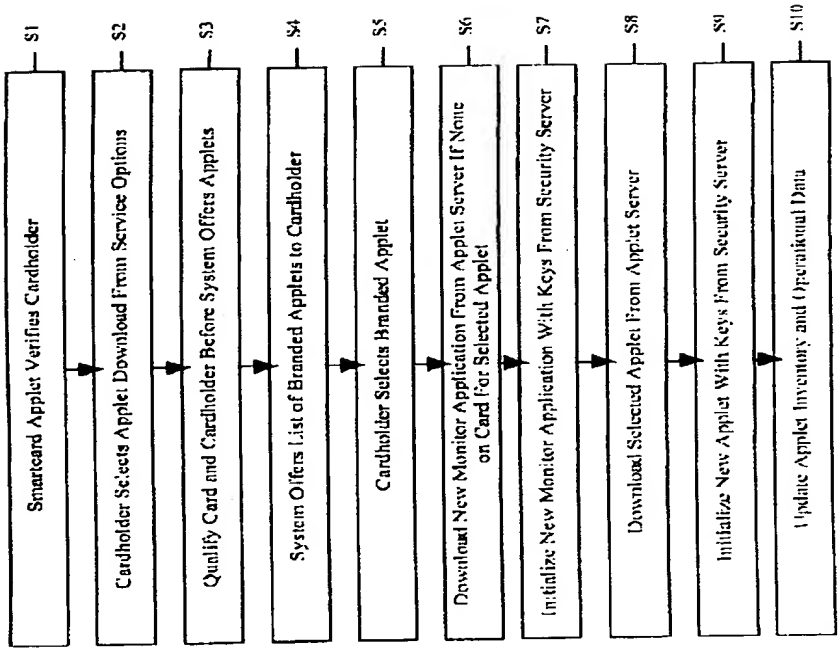

S1
Smartcard Applet Verifies Cardholder
S2
Cardholder Selects Applet Download From Service Options
S3
Qualify Card and Cardholder Before System Offers Applets
S4
System Offers List of Branded Applets to Cardholder
S5
Cardholder Selects Branded Applet
S6
Download New Monitor Application From Applet Server If None on Card For Selected Applet
S7
Initialize New Monitor Application With Keys From Security Server
S8
Download Selected Applet From Applet Server
S9
Initialize New Applet With Keys From Security Server
S10
Update Applet Inventory and Operational Data

FIG. 4

ABSTRACT

A method and system for managing applications for a multi-function smartcard makes use of a resident master application and one or more monitor applications installed on the smartcard microcomputer to authorize downloading of new applications to the smartcard and to manage applications on the smartcard. New applications are installed on the smartcard using a security mechanism of the monitor application. When a new application is installed, it is provided, for example, with an operation key, cardholder information, and a digital certificate. The new application is registered in a software registry of the smartcard according to an object-oriented classification, a copy of the registry is stored in an electronic deposit box, and the electronic deposit box is updated with operational data for the new application. The new application selectively shares one or more objects with objects of other applications on the smartcard on a restricted or unrestricted basis.

T0091-171368
WINLIB01:725062.01